FEDERAL STUDENT AID

We Help Put America Through School

FSA Technology Policies, Standards & Products Guide

Version 4.0

August 1, 2003

Business Technology Alignment

TABLE OF CONTENTS

DOCUMENT REVISION HISTORY

Version No.	Date	Author	Revisions Made
1.0	November 2, 2001	Paul Smith	Provided general updates under TO 55.
2.0	January 25, 2002	Karen Anderson, Bill Malyszka	Reformatted document to align with the Department of Education Policy document and updated document to reflect new standards and products.
2.1	February 12, 2002	Karen Anderson, Bill Malyszka, David Elliott	Updated document with client feedback. Renamed document title.
2.2	March 29, 2002	Karen Anderson, Bill Malyszka, David Elliott	Included updates from 1/15/2002 to 3/15/2002 in FSA standards, products, and policies. Added an Application Development section.
2.3	June 30, 2002	Bill Malyszka, David Elliott	Incorporate planned ITA upgrades, added an executive summary, added Mobile Devices to Network Services section, added External Connections to External Environment section, and updated several version numbers.
3.0	September 27, 2002	Bill Malyszka, David Elliott	Updated to include minor version number changes and other architectural changes. Reflects all updates through revision date.
3.1	April 1, 2003	Reza Sahami David Elliott	Updated to include minor version number changes and other architectural changes. Reflects all updates through revision date.
4.0	August 1, 2003	W. Terry Hardgrave Nanatu Scott Deb White Denise Hill	Updated to include minor version number changes and other architectural changes. Reflects all updates through revision date.

EXECUTIVE SUMMARY

The *FSA Technology Policies, Standards, and Products Guide* describes the Federal Student Aid (FSA) enterprise-wide architecture standards. The policies, standards, and products selected by FSA enable the organization to leverage common components of the architecture to realize cost savings and accumulate skills and knowledge around the common components. The selected policies, standards, and products satisfy external requirements while enabling the integration of FSA system applications.

User Interface (p. 14)	*Web Browsers*	HTML 4.0, HTTP 1.1
	Portals	IBM WebSphere Custom Components (Reusable Common Services (RCS components) and Projects)
	Computer Telephony Integration / Interactive Voice Recognition	Genesys, Cisco
	Audio Graphic Conferencing	TBD
	Text-Based Conferencing	TBD
	Video Conferencing	Picturetel, CritiCom (H.323, H.320)
	Emulation	Attachmate, Hummingbird XCeed 6.1
Application Services (p. 19)	*Desktop Tools*	MS Office 2000 Professional, MS Internet Explorer 5.5, MS Outlook 2000
	Component Broker	IBM WebSphere/IIOP
	Knowledge Management	Autonomy Knowledge Suite 3.1
	Enterprise Application Integration (EAI)	IBM MQSeries Workflow 3.2.2
	Business Process Management (BPM)	IBM MQSeries Workflow 3.2.2
	Content Management	Interwoven Teamsite 5.5, Interwoven OpenDeploy 5.5
	Search Engine	Autonomy Knowledge Suite 3.1
	Business Services	Oracle Federal Financial 11.03, Siebel Enterprise Application Gateway 5.6
	Mail Servers	MS Exchange 2000, Sendmail
Enterprise Data Management (p. 25)	*Metadata Management*	TBD
	Data Modeling	Rational Rose 2001a, Sybase Power Designer, Computer Associates CoolGen 5.1
	Database Management	Oracle 8i 8.1.7, IBM DB2
	Data Acquisition	Informatica Power Center Server 5.2
	Data Warehousing Technologies	MicroStrategy 7i, Intelligence Server 7.2, Web 7.2, Narrowcaster 7.2, Agent 7.2, Architect 7.2, Crystal Reports 8.0, WebFOCUS
	Imaging	Optika Accorde Suite, IBM Image Plus
	Enterprise Architecture Management	Popkin System Architect 9.1

Distributed Computing (p. 31)	*Application Server*	IBM WebSphere Enterprise Edition 3.5.5/5.0, Oracle Application Server 8.0
	Web Server	IBM IHS Server 1.3.26, Microsoft IIS 4.0
	Web Server Monitoring	WebTrends Enterprise Reporting Server 3.6, SAS
	Middleware	IBM MQSeries Server 5.2, IBM MQSeries Client 5.2
	Application Specific	J2EE Compliant
Data Interchange (p. 36)	*XML Server*	Innovision XML Server
	File Transfer	FTP, HTTP, SMTP, CommerceQuest Data Integrator 4.0.1, FTAM, SNA
	Electronic Data Interchange	XML, bTrade
	File Compression	Compress, WinZip 8.0
Network Services (p. 39)	*Application Directory Services*	LDAP, Netscape Directory Server
	Transfer Protocol	TCP/IP, SNA
	Application Gateway	CA Java Proxy, CA COMM Proxy
	Network Address Management	DHCP, Static IP, NAT
	Naming Services	DNS
	Remote Access Services	Cisco Secure RADIUS, Citrix
	Virtual Private Network	CheckPoint VPN-1
	Physical Layer	Ethernet
	Wireless Devices	Blackberry 2.1
Operating Systems (p. 44)	*Mainframe*	OS/390 MVS 2.11, CICS
	Mid Tier	HP/UX 11, HP/UX 10.20, MS Windows NT 4, MS Windows 2000, Sun Solaris 2.6/2.8
	Personal Computers	MS Windows 2000
	Mobile Devices	PalmOS 4.0
Application Development (p. 47)	*Application Design*	Rational Rose 2002
	Programming Tools	IBM WebSphere Studio Application Developer (WSAD) 5.0, Sun Java Development Kit 1.3, Oracle JDeveloper, Computer Associates CoolGen 5.1
	Application Testing	Mercury Interactive Loadrunner, Rational TestManager
	Code Management	Rational ClearCase 4.1, Rational ClearQuest 2001, Computer Associates Harvester Change Manager, Computer Associates Endeavor, Microsoft Source Safe

System Management (p. 50)	*Configuration Management*	Rational ClearCase 4.1, Rational ClearQuest 2001, Computer Associates Harvester Change Manager, Computer Associates Endeavor, Microsoft Source Safe
	Inventory Management	Custom Solution
	Operations Management	Computer Associates CA-7, BMC Control D 3.5, BMC Control M/R, HP OpenView 3.5, Computer Associates UniCenter TNG 2.4
	Load Balancing	IBM Network Dispatcher 4.0, Cisco Local Director, HP Service Guard
	Network Inventory and Distribution Services	MS Software Management System, Candle Management, Lotus Notes
	Capability Maturity Model (CMM)	See Website at www.sei.cmu.edu
Security Services (p. 54)	*Digital Certificate Services*	Netscape Certificate Server
	Firewall Services	CheckPoint Firewall-1
	Access Control	IBM RACF, BMC Control SA, Computer Associates UniCenter TNG
	Directory Access	LDAP
	Audit Trail Creation	System Log File
	Authentication	IBM RACF, Computer Associates UniCenter TNG 2.4, Oracle 8i 8.1.7, FSA Pin, BMC Control SA
	Database Security Services	IBM RACF, Oracle 8i 8.1.7, Top Secret
	Electronic Signatures/Non-repudiation	TBD
	Host Intrusion Detection	Tripwire 2.4.2
	Network Intrusion Detection	RealSecure/CheckPoint
	Physical Security	OMB A130
	Encryption	Router Encryption (DES3), IPSec, Verisign 3.0, RSA Bsafe, RSA Bsafe Libraries, Sterling Commerce Connect Direct
	Virus Protection	McAfee VirusScan, Norton Antivirus 7.1
External Environment (p. 64)	*External Connections*	Asynchronous Transfer Mode (ATM), Inverse Multiplexed Circuits (IMUX), Frame Relay, Point-to-point, Virtual Private Network (VPN)

1 INTRODUCTION

This document is a reference tool for Federal Student Aid (FSA) technical architects, system administrators, application developers, procurement personnel, and others that require guidance on implementing FSA technical standards, standard products, and policies.

The current version of this document includes all changes made through August 1, 2003.

1.1 Using this Guide

The *FSA Technology Policies, Standards & Products Guide* covers various service areas including User Interface Services, Application Services, Enterprise Data Management, Distributed Computing, Data Interchange, Network Services, Operating Systems, Application Development, System Management, Security Services, and External Environment. The following information appears for each service in a service area:

- *Brief Description* defines a service and describes its functionality.
- *Target Standards* appear in a table that contains the current and planned FSA solution standards. These standards include the forecast for each product and standard over three Federal fiscal years.
- *Approved Standards* provide a detailed description of policy underlying each technical standard or standard product and the rationale for the selection of a standard or product.

Each product and standard listed in this guide falls into a category such as a technical standard, a standard product, or a de facto product. The following defines each category:

- *Technical Standards* are industry standards that FSA has adopted for all use in implementing systems except when a business or technical need requires an exception to the standard.
- *Standard Products* are solutions that FSA has selected for future development and implementation. Exceptions to the use of a standard product are made when there is a strong business or technical case to deviate.
- *De Facto Products* are included in the FSA environment for a particular project requirement but have not been adopted as enterprise-wide standards. De facto products serve as the starting point for selecting a product for use on a project when there is no FSA standard product.

1.2 Sources of Standards and Policies

The technology policies standards and products apply throughout the U.S. Department of Education Federal Student Aid (FSA) systems enhancement effort. The FSA architecture is

based on The Open Group Architectural Framework (TOGAF) which defines a process for developing an architecture and describes the fundamental technologies in the architecture.

FSA employs both open systems standards and proprietary standards. Open systems products and technologies use open interfaces with specifications that are readily available to the public and revised with timely notice through a public process. Proprietary standards are not publicly available and may be implemented through commercial off the shelf (COTS) products or developed by FSA.

FSA strives to comply with external policies and standards as established in legislation and federal government policy. In particular, FSA is following compliance with Clinger-Cohen legislation in addition to the Office of Management and Budget guidelines on Federal Enterprise Architecture (FEA). The FEA work includes development of several FEA Reference Models (i.e. BRM, PRM, SRM, DRM, TRM) for each major Information Technology initiative.

1.3 Authority and Governance

The authority for the *FSA Technology Policies, Standards & Products Guide* comes from the FSA Chief Information Officer through the Information Technology (IT) Management organization. The roles, responsibilities, and IT decision-making processes within FSA collectively referred to as Enterprise Architecture Management (EAM) appear in Section 8 of the *FSA Information Technology Architecture Framework – Phase I* document. Changes and additions to these standards are made through the Architecture Working Group that follows the Business-Technology Alignment (BTA) process. For more information on the Architecture Working Group or the BTA process, contact Denise Hill the FSA Chief Architect at 202-377-3030.

2 CONCEPTUAL ARCHITECTURE

This *FSA Technology Policies, Standards, & Products Guide* complements the FSA Technology Architecture (TA). The TA provides the framework of principles and practices that direct the design, construction, deployment, and management of information technology and systems (from *Enterprise Information Technology Architecture Framework: Business Drivers and Architecture Principles* October 8, 1998). The guiding principles are:

- *The architecture must support the business.* The enterprise architecture and standards will (1) support and optimize FSA operations, (2) be highly flexible to accommodate future business changes, and (3) help ensure the overall success of the FSA business.
- *Reengineer business processes and supporting IT together.* The implementation of new information systems will proceed after work processes have been analyzed, simplified, or otherwise redesigned in compliance with Clinger-Cohen legislation and Raines' rules.
- *Enhance and simplify access to information.* Timely access to information through the tools and applications required to access and manipulate that information will be available to all individuals unless there is a specific, compelling reason to restrict access.
- *Design integration and reuse into IT initiatives.* FSA IT initiatives will maximize reuse of existing code and databases.
- *Use industry-proven technology.* IT applications and technical infrastructure decisions will use industry-proven and supported components, methods, standards, and tools consistent with industry technological and market direction.
- *Maintain vendor neutrality.* Standards and technology choices will be based on vendor-neutral standards where they are available and realistically can be implemented. Products will be chosen from any vendor that has strong business stability, provides the best technology and service for a business need, and whose products are compliant with architecture standards.
- *Solutions preference.* When most cost effective and beneficial, FSA's solutions preference will be (1) outsourcing, (2) commercial-off-the-shelf (COTS) products, (3) reuse of existing applications, and (4) custom applications.
- *Reduce integration complexity.* Products, tools, designs, applications, and methods will be selected to reduce integration and infrastructure complexity.
- *Architecture enforcement.* The information systems and technology infrastructure implemented by FSA will be compliant with the FSA Enterprise Architecture and Common Operating Environment (COE).
- *Periodic architecture review, alignment, and refreshment*. The TA will be periodically reviewed (at least annually) and updated according to a disciplined, structured maintenance and technology refreshment process. This structure will include a configuration management process and supporting tools.

2.1 Federal Enterprise Architecture (FEA)

The Federal Enterprise Architecture (FEA) is a tool that enables the federal agencies to identify opportunities to leverage technology and alleviate redundancy, or to highlight where agency overlap limits the value of IT investments.

As a Performance-Based Organization (PBO), FSA has a unique opportunity to leverage the FEA work to accomplish FSA goals to improve accountability and to continue to reduce costs in implementing the FSA mission.

Led by the Office of Management and Budget (OMB), the purpose of the FEA is to identify opportunities to simplify processes, re-use Federal IT investments and unify work across the agencies and within the lines of business of the Federal Government. The outcome of this effort will be a more citizen-centered, customer-focused government that maximizes technology investments to better achieve mission outcomes. As illustrated in Exhibit 2-1, FEA is comprised of five reference models (PRM, BRM, SRM, TRM, and DRM). The models facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal Agencies.

The Performance Reference Model (PRM) is a framework of performance measurement that provides common outcome and output measures throughout the Federal government. It allows agencies to better manage the business of Government at a strategic level while providing a means for gauging progress towards the target FEA.

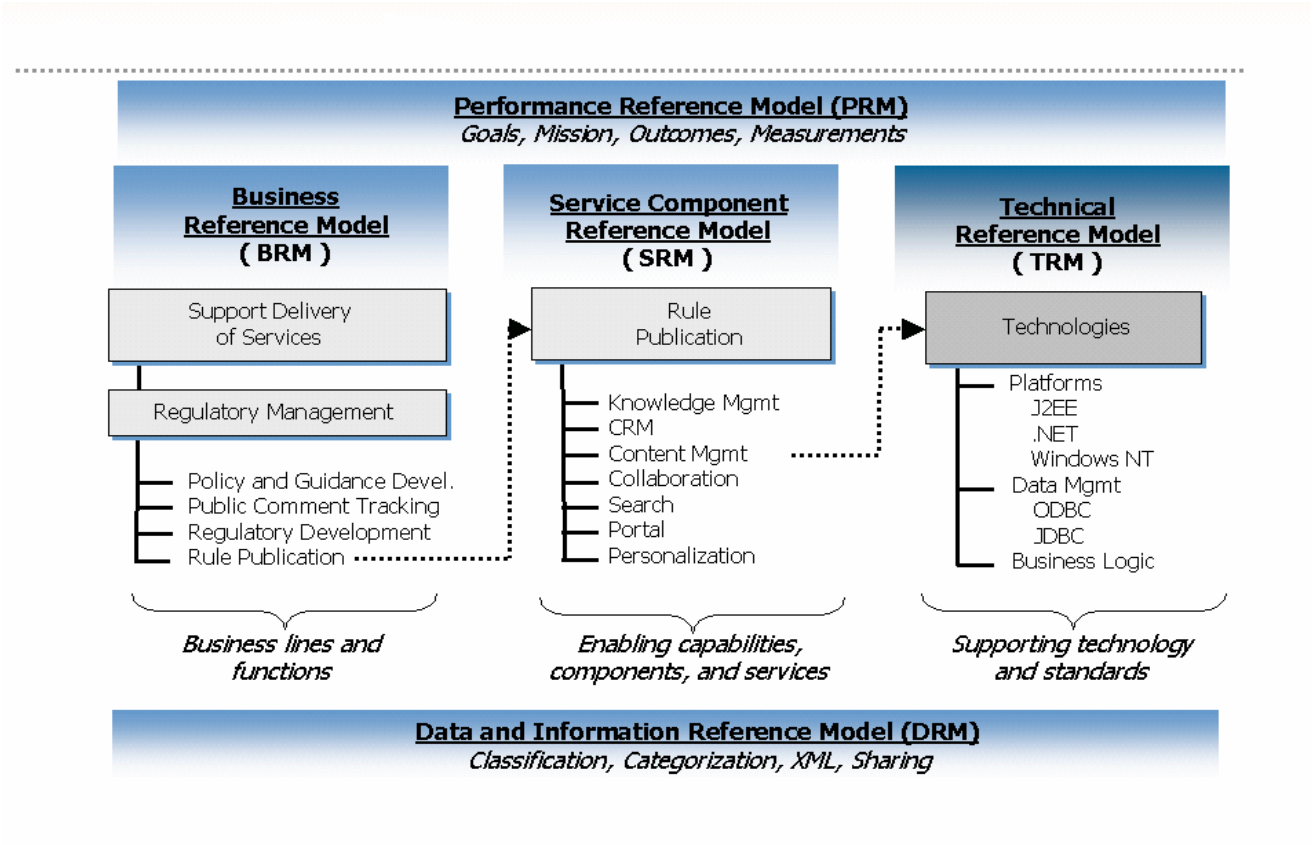
The Business Reference Model (BRM) serves as the foundation for FEA and it is the main viewpoint for the analysis of data, service components and technology. The model describes the Federal Government's Lines of Business (LOB), including operations and services for the citizen.

The Service Reference Model (SRM) is a business-driven, functional framework that classifies service components according to business and/or performance objectives.

The Technical Reference Model (TRM) describes how technology supports the secure delivery, exchange, and construction of service components.

The Data and Information Reference Model (DRM) is still being developed. It will describe at an aggregate level, the data and information that support program and business line operations. The model will aid in describing the types of interactions and information exchanges that occur between the Federal Government and its various customers, constituencies, and business partners.

Exhibit 2-1: FEA Integrated Model Conceptual View



3 TECHNICAL REFERENCE MODEL

The basis for the Technology Policies, Standards, & Products Guide is the Technical Reference Model (TRM), which is a conceptual representation of services and interfaces in information systems. The FEA TRM as depicted in Exhibit 3-1 is a component-driven, technical framework that identifies the standards and specifications that comprise a service component. The TRM describes how a component is accessed, built, deployed, and maintained.

Exhibit 3-1: FEA Technical Reference Model (TRM)

Service Access and Delivery			
Access Channels	**Delivery Channels**	**Service Requirements**	**Service Transport**
Web Browser	Internet, Intranet	Legislative/Compliance	Network Services
Wireless/PDA Device	Extranet	Authentication/Single Sign-On	Transport
Collaboration/Communication	Peer to Peer (PIP)	Hosting	
Other Electronic Channels	Virtual Private Network (VPN)		
Service Platform and Infrastructure			
Support Platforms	**Delivery Servers**	**Hardware/Infrastructure**	
Wireless/Mobile	Web, Media	Servers/Computers	
Platform Independent (J2EE)	Application	Embedded Technology Devices	
Platform Dependent (.NET)	Portal	Peripherals	
		WAN, LAN	
Database/Storage	**Software Engineering**	Network Devices/Standards	
Database	Integrated Development Environment (IDE)	Video Conferencing	
Storage Devices	Software Configuration Management (SCM)		
	Testing Management, Modeling		
Component Framework			
Security	**Presentation/Interface**	**Business Logic**	**Data Management**
Certificate/Digital Signature	Static Display	Platform Independent	Database Connectivity
Supporting Security Services	Dynamic Server-Side Display	Platform Dependent	Reporting and Analysis
	Content Rendering		
Data Interchange	Wireless/Mobile/Voice		
Data Exchange			
Service Interface and Integration			
Integration	**Interoperability**	**Interface**	
Middleware	Data Format/Classification	Service Discovery	
Database Access	Data Types/Validation	Service Description/Interface	
Transaction Processing	Data Transformation		
Object Request Broker			

The TRM includes four (4) core Service Areas. Service Areas represent a technical tier supporting the secure construction, exchange, and delivery of Service Components. Each Service Area aggregates and groups the standards, specifications, and technologies into lower-level functional areas. There are four (4) Service Areas within the TRM:

- ***Service Access and Delivery -*** refers to the collection of standards and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific Service Component.

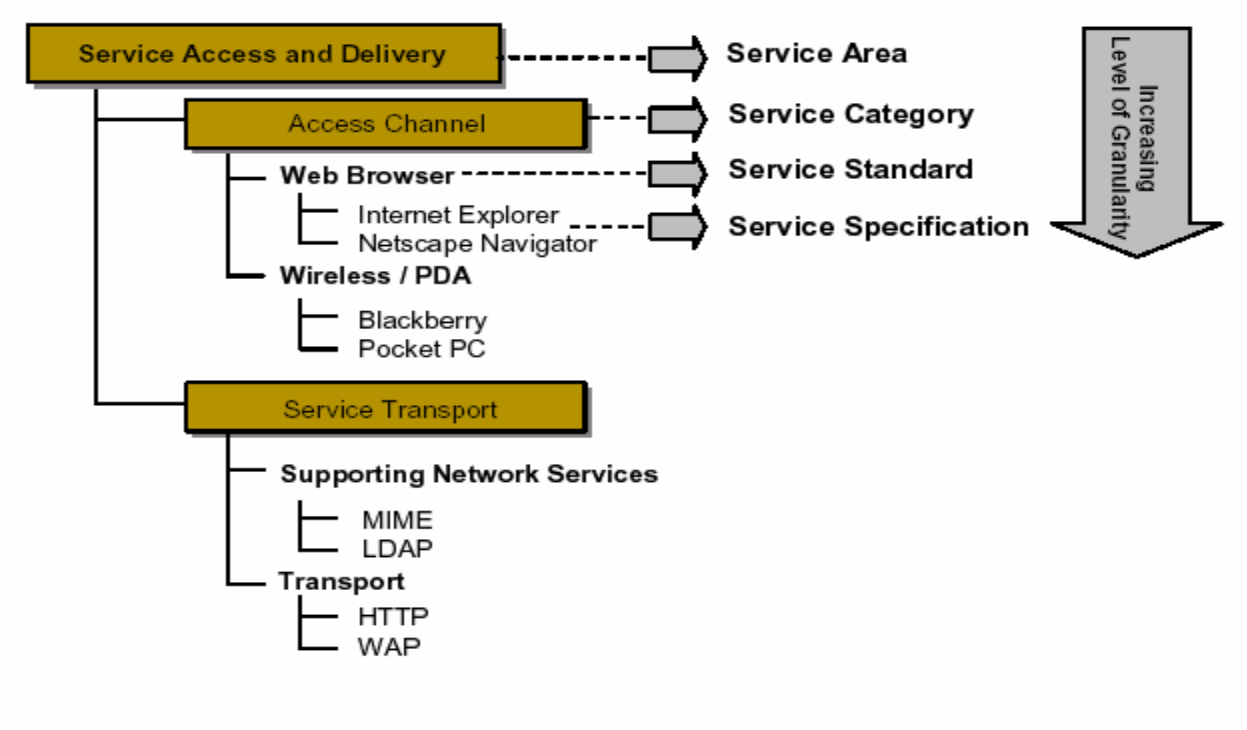
- ***Service Platform & Infrastructure -*** refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

- ***Component Framework*** - refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Component-Based, Distributed, or Service-Orientated Architectures.

- ***Service Interface and Integration -*** refers to the collection of technologies, methodologies, standards, and specifications that govern how agencies will interface (both internally and externally) with a Service Component. This area also defines the methods by which components will interface and integrate with back office / legacy assets.

Each Service Area, as illustrated in Exhibit 3-2, consists of multiple Service Categories, Service Standards, and Service Specifications that provide the foundation to group standards, specifications, and technologies that directly support the Service Area.

Exhibit 3-2: Service Categories, Service Standards, and Service Specifications



Visit the following Federal Enterprise Architecture Program Management Office (FEAPMO) website to get more information about TRM: **http://www.feapmo.gov/fea_downloads.asp**

4 TECHNOLOGY POLICIES, STANDARDS & PRODUCTS

This section addresses the major service areas of the architecture. A discussion of each of the following exists for each service area:

- Description of the service
- Target standards
- Description of the technology policy for each standard and product
- Rationale for each standard and product

The table shows the target standards listing the products used by FSA now and those slated for future use. For each product, the type of standard also appears. FSA updates the tables on a quarterly basis to reflect changes in its business objectives and emerging technologies.

4.1 User Interface Services

Brief Description

User interface services provide the means for users to interact with applications. Depending on the capabilities required by users and the applications, these interfaces may include the following:

- *Web browsers* are client applications that provide a user interface by rendering Hypertext Markup Language (HTML) documents. They allow users to view and interact with applications and documents containing text, graphics, audio, and other content. Web browsers also provide support for navigation within and across documents through the use of embedded hyperlinks. Technologies such as Java allow users to interact with existing legacy applications through web browsers.
- *Portals* provide a web-based user-customizable point of access to a wide variety of content, documents, and applications. A portal provides integrated access, authorization, and authentication to FSA services through the web.
- *Computer Telephony Integration (CTI)* merges computers, networks, PBX switches, PC-based answering machines, faxes, and pagers. CTI enables automated handling of telephone calls, automatic call back, initiation of workflow, a high quality of service for customers, and sophisticated task tracking.
- *Audio Graphic Conferencing* provides a cost-effective method of conferencing when seeing the conference participants is not essential. The audio is typically a telephone conference call,

and a whiteboard image is provided over the network that can be modified by all participants. The whiteboard enables collaboration beyond a telephone conference call.

- *Text-Based Conferencing* allows conference participants to view each other's text input. One of the features of the text-based conference is that the text can be saved and referred to at a later time. It requires the lowest network bandwidth of the three types of conferencing described.
- *Video Conferencing* enables people at different sites to simulate face-to-face meetings in real time. Current video conferencing options range from stationary systems installed in dedicated video conferencing rooms to personal computer video units. In addition to voice and video, video conferencing systems may enable the sharing of graphics and electronic documents. Personal computer video conferencing links individuals rather than groups.
- *Emulation* provides a means to access remote computers and to work on one platform from a different platform. These services can provide either Graphic User Interface (GUI) or character-based access to remote systems.

Target Standards

Target Standards: User Interface

	FY 2003	FY 2004	FY 2005
Web Browsers			
Technical Standard	HTML 4.0	HTML 4.0	HTML 4.0
Technical Standard	HTTP 1.1	HTTP 1.1	HTTP 1.1
Portals			
De Facto Product	IBM WebSphere Custom Components (Reusable Common Services (RCS components) and Portlets)	IBM WebSphere Custom Components (Reusable Common Services (RCS components) and Portlets)	IBM WebSphere Custom Components (Reusable Common Services (RCS components) and Portlets)
Computer Telephony Integration/Interactive Voice Recognition			
Standard Product	Genesys	Genesys	Genesys
De Facto Product	CISCO (VoIP Automated Call Distribution Software)	CISCO (VoIP Automated Call Distribution Software)	CISCO (VoIP Automated Call Distribution Software)
Audio Graphic Conferencing			
	TBD	TBD	TBD
Text-Based Conferencing			
	TBD	TBD	TBD
Video Conferencing			
Standard Product	CritiCom (H.323, H.320)	CritiCom (H.323, H.320)	CritiCom (H.323, H.320)
De Facto Product	PictureTel	PictureTel	PictureTel

Emulation			
Standard Product	Attachmate	Attachmate	Attachmate
Standard Product	Hummingbird XCeed 6.1	Hummingbird XCeed 6.1	Hummingbird XCeed 6.1

Approved Standards

Web Browsers – HTML 4.0, HTTP 1.1

Description: FSA web browser services will provide server communication, communication security, Section 508 accessibility, presentation services, scripting, and run-time services. FSA products should support HTML and Java technologies.

Rationale: For external users accessing FSA information via a web browser, FSA language and protocol standards are HTML v4.0 and HTTP v1.0. FSA customers will use a variety of browsers, including text-based browsers such as Lynx. Support does not imply full functionality of features that are available only with more recent products.

Portals –WebSphere Custom Components

Description: Portal technology will provide a single point of access to FSA data and will be implemented with WebSphere Custom Components to provide the portal services. Re-usable Common Services (RCS) as a part of the Integrated Technology Architecture (ITA) project provides components.

Rationale: No published industry standard identified.

RCS Components are:

- Mail Framework: Provides a simple and robust email framework that can easily be utilized by any FSA development team.
- Search Framework: Simplifies, standardizes, and improves the use of FSA's standard search engine (Autonomy).
- Logging Framework: IBM Websphere Application Server has limited logging functionality, thus the RCS logging framework was developed to provide a more robust, functional, and customizable logging facility.
- Exception Handling Framework: Java has its own exception class that gives the generic error messages for a variety of errors. This framework was developed to give more accurate, customizable error messages.
- Persistence Framework: Provides flexible mapping of the business

objects to relational database tables.

- Component Factory: To hide object creation from its usage – to allow users to decouple object creation from its use.
- Configuration Framework: Improves setup and access to application-wide configuration data.
- Web Conversation Framework: Standardizes web application development using Servlets and Java Server Pages (JSPs).
- Session Framework: Maintains user state and context information as the user navigates from one page to another.
- XML Helper Framework: To facilitate different XML parsing mechanisms for Java developers.
- FTP Framework: Enables Java developers to implement file transfer capabilities in web applications.
- Scheduler Framework: To setup and execute scheduled jobs from Java applications.
- JSP Tag library: Utilities to be used in Java Server Pages (JSPs) to facilitate tedious, repetitive tasks and reduce development costs.
- SOAP Framework: Simplifies and standardizes the exchange of data via XML format over HTTP.

Portlets:

- Calendar: Displays a tabular calendar view and detail for the selected day
- Logon: Authenticates registered users
- Registration: Allows either a new user to create a new registration and logon or a currently logged-on user to edit their registration information.
- Personalization: Allows a new user to register, or an existing user to modify personal information.
- Headlines: Displays current FSA headlines
- Search: Allows simple search or advanced search using Autonomy
- Feedback: Allows users to provide feedback through a configuration survey

Rationale: No published industry standard identified. Components are written in Java to J2EE standards to work with any J2EE-compliant application server.

Computer Telephony Integration (CTI) / Interactive Voice Recognition – Genesys, CISCO

Description: FSA continues to align its customer relationship management CRM solutions, which will include CTI, with industry best practices.

Rationale: Industry standards vary by platform; more detail will be provided as the standards are selected.

Audio Graphic Conferencing – TBD

Description: To be determined.

Rationale: Multiple industry standards exist. No recommendation has been made.

Text-Based Conferencing – TBD

Description: To be determined.

Rationale: Multiple industry standards exist. No recommendation has been made.

Video Conferencing – CritiCom (H.323, H.320), PictureTel

Description: The CritiCom video bridging system supports connecting multiple sites together through the H.323 or H.320 standards.

Rationale: H.323 and H.320 are multimedia standards related to video conferencing. They are both distributed by the ITU.

Emulation –Attachmate (TN3270), Hummingbird XCeed 6.1 (X Windows, Telnet)

Description: FSA will use emulation to access remote systems. Specifically, X Windows will be used to provide a GUI interface to Unix applications, Telnet will provide character-based access to remote systems, Attachmate provides TN3270, TN3274, telnet, and FTP. Hummingbird XCeed provides Xterm, FTP, and telnet access. Hummingbird Maestro, which is a subset of the XCeed product, provides network file system (NFS) connectivity to remote drive partitions.

Rationale: FSA technical standards and standard policies are based on established industry

standards.

4.2 Application Services

Brief Descriptions

Application services provide support for the business processes of an organization including transaction services. These services also enable an organization to deploy network-centric applications in the internet and intranet environments encompassing both application server services and web server services.

The FSA Desktop COE, cited in this and following sections, is defined as the commercial-off-the-shelf (COTS) products and applications supported by the Microsoft Office 2000 suite of products in the current FSA Seat Management project.

- *Desktop Tools* are office productivity applications that support a standard office automation environment. They include user interface, word processing, spreadsheets, presentation graphics, and web browsers.
- *Component Brokers* provide object-based functionality to the application server. An object-based capability provides a standard model for object state and behavior accessible through object methods. A component broker provides a scalable, manageable environment for developing and deploying distributed component-based solutions. The component broker is an object server that includes a development environment that is optimized for creating business objects that run in the component broker server. This server consists of both a run-time package and a development environment.
- *Knowledge Management* provides information search and retrieval capability and may provide automated management of hyperlinks. These services offer various search types on different data groups, such as unstructured digital information, structured data, word processing documents, HTML-based files, e-mail messages, and electronic news feeds. Knowledge management may also provide software that attempts to classify and cluster knowledge about various topics or automatically create hyperlinks among related documents.
- *Business Process Management* facilitates work-related processes within an organization and often supports relatively static business processes, such as purchase order processing and claims processing. Workflow management creates run-time options by navigating through previously defined workflow models. Applications are invoked automatically, and work items are created and distributed to the people involved. Mail systems, groupware tools, and electronic forms packages can also provide some workflow functionality.
- *Content Management* manages web site content delivery from the development environment to the production environment. The content management component provides the following services:

Authoring—allows users to associate and launch development applications against the content managed by the component.

Versioning—maintains versions of each individual web site artifact. The individual content versions are associated with web site configurations or releases.

Categorization and Publishing—manages groups of content artifacts according to user-defined criteria and supports publishing of these content artifacts.

Development Collaboration and Workflow—provides process control and related methods that support collaboration between personnel in the development community and the production community. The collaboration and workflow utilities provide a methodical way to ensure that content change is appropriately authorized.

Integration of Multiple File Types—supports any type of file.

Summarization—produces a summary report of a configuration or release and the web site artefacts that were delivered from the development environment to the production environment.

- *Search Engines* provide search and retrieval capability on different data sets in an internet-based environment.
- *Business Services* provide specific support for business processes such as financial management and customer relations management (CRM).
- *Mail Servers* provide the ability to transport email to and from individuals and applications.

Target Standards

Target Standards: Application Services

	FY 2003	FY 2004	FY 2005
Desktop Tools			
Standard Product	Microsoft Office 2000 Professional	Microsoft Office 2000 Professional	Microsoft Office 2000 Professional
Standard Product	Microsoft Internet Explorer 5.5	Microsoft Internet Explorer 6.0	Microsoft Internet Explorer 6.0
Standard Product	Microsoft Outlook 2000	Microsoft Outlook 2000	Microsoft Outlook 2000
Component Broker			
Standard Product	IBM WebSphere 3.5.5/IIOP	IBM WebSphere 5.0/IIOP	IBM WebSphere 5.0/IIOP
Knowledge Management			
Standard Product	Autonomy Knowledge Suite 4.3.3	Currently being evaluated.	TBD

Business Process Management (BPM)			
Standard Product	IBM MQ Series Workflow 5.2	IBM MQ Series Workflow 5.3	IBM MQ Series Workflow 5.3
Content Management:			
Standard Product	Interwoven Teamsite 5.0.1	Interwoven Teamsite 5.2	Interwoven Teamsite 5.2
Standard Product	Interwoven OpenDeploy 5.0.1	Interwoven OpenDeploy 5.2	Interwoven OpenDeploy 5.2
Search Engine:			
Standard Product	Autonomy Knowledge Suite 4.3.3	Google	Google
Business Services			
Standard Product	Oracle Federal Financials 11i	Oracle Federal Financials 11.0.3	Oracle Federal Financials 11.0.3
Standard Product	Siebel Enterprise Application Gateway Server 5.6	Siebel Enterprise Application Gateway Server 5.6	Siebel Enterprise Application Gateway Server 5.6
Mail Servers			
Standard Product	Microsoft Exchange 2000	Microsoft Exchange 2000	Microsoft Exchange 2000
Standard Product	Sendmail	Sendmail	Sendmail

Approved Standards

Desktop Tools – MS Office 2000 Professional, MS Internet Explorer 5.5

Description: The FSA Desktop Common Operating Environment (COE) specifies the desktop tools. The FSA standard office productivity tool standard consists of programs for word processing, spreadsheet, and presentation graphics. Software products that are designed to international or national standards are preferred over those designed to a lower standard. Additionally, COTS software is always preferred over government-off-the-shelf (GOTS) software produced by other federal agencies or private companies working under contract for the government.

Rationale: Standards for common office productivity tools are typically defined by de facto industry file formats. File formats are formal structures of file records and layouts that are recognizable and usable by various related products. As a product becomes prominent in the industry, other tools and products tend to include the capability to access, use, and create files in the same format as those used by the prominent product. Common file formats for standard office and other productivity tools are given in the table below.

Document Type	Standard/Vendor Format	Recommended File Name Extension
Plain Text	ASCII Text	.txt
Compound	Acrobat	.pdf

Document	HTML	.htm
	Extensible HTML	.xhtml
	MS Word	.doc
	Rich Text Format	.rtf
Presentation	MS PowerPoint	.ppt
Spreadsheet	MS Excel	.xls
Graphics	CGM	
	JFIF	
	GIF	.gif
Audio	Wave	.wav
	Audio-Video Interleaved	.avi
	Audio UNIX	.au
Video	MPEG, MPEG2	.mpe, .mpg
	Real Video	.rm, .ram
Internet	HTML	.htm
Compressed	WINZip	.zip
Database	Dbase	.dbf
	MS Access	.mdb

Component Broker – IBM WebSphere 3.5.5/IIOP

Description: The FSA component broker application will transparently provide a number of services to business objects or enterprise beans, including concurrency control, event, notification, externalization, identity, naming, transaction, query, and security services. The component broker run-time environment will support the execution of C++ and Java-based business logic that follows the CORBA 2.0 model or the EJB 2.0 specification.

Rationale: FSA component broker standards will comply with the open standards contained in the Object Management Group's (OMG) Common Object Request Broker Architecture (CORBA) initiative and the Component Broker Managed Object Framework (MOFW).

IBM WebSphere 3.5.5 will be upgraded to version 5.0 this summer (2003).

Knowledge Management – Autonomy Knowledge Suite v4.3.3

Description: The FSA knowledge management function, in conjunction with the search engine function, will provide a technology infrastructure for the automatic

leveraging of content. This will provide the ability to use various types of information searches and personalized profiling and features to search both structured and unstructured data. The FSA product will support a thesaurus query if a thesaurus is loaded into the environment.

Rationale: No published industry standard identified.

Search Engine – Autonomy Knowledge Suite v4.3.3

Description: The search engine will provide pattern-matching technology that will enable FSA to efficiently identify and encode unique key words within text documents. The search engine will then locate and retrieve content, such as a set of web sites, news feed, or an e-mail archive that match the search parameters.

Rationale: No published industry standard identified.

Business Process Management (BPM) – MQ Series Workflow v5.2

Description: BPM is a collection of tools for modeling the enterprise business processes. They may also be useful for performing activity-based costing, simulating the processes and deploying them. FSA will use BPM tools to design, document, execute, control, improve, and optimize the business processes. FSA will leverage the tools to provide the following:

- Core components of the enterprise architecture through integration of business processes across enterprises by acting as a workflow broker.
- Integration of existing CICS applications to power e-business solutions
- Management of fully automated application-to-application workflow
- Management of workflow processes, including applications that require human intervention
- Web browser support with rapid application integration capability
- Scalability from Windows NT up to IBM OS/390 MVS servers

Rationale: No BPM standards currently exist, but the Workflow Management Coalition (WfMC) is defining standard interfaces between workflow engines, workflow definition packages, management information tools, work list tools, and invoked applications. FSA workflow applications should use high-level application programming interfaces (APIs) to communicate with desktop

applications and use industry-standard relational databases as their data store.

IBM MQ Series Workflow 5.2 will be upgraded to version 5.3 this summer (2003).

Content Management – Interwoven Teamsite v5.0.1, Interwoven OpenDeploy v5.0.1

Description: Content management will accelerate the way FSA delivers its business to the web, leveraging appropriate resources at all levels of the organization. Distributed control over content creation and deployment will shorten the launch cycle by enabling the management of the process. Content management will include replication and syndication features with rules-based distribution of all content across the FSA network. It will manage numerous deployment rules for FSA web sites. These deployment rules will support automated processes such as one-button publishing and transformation processes such as deployment to web configurations.

Rationale: No industry standard is established.

Interwoven 5.0.1will be upgraded to version 5.2 this summer (2003).

Business Services – Oracle Federal Financial System 11i, Siebel Enterprise Application Gateway 5.6

Description: FSA will utilize COTS to implement business processes through application systems implementing business services. The specific requirements of the business process will drive the selection and configuration of a COTS solution.

The Oracle Federal Financial System will manage the flow of all financial information through FSA. It will give the CFO office the ability to report information across programs, consolidate redundant processes, and account for FSA Title IV funds.

Siebel Enterprise Application Gateway will be used as FSA's Customer Interaction Application to enable delivery of a seamless customer experience at any touch point across multiple communication methods.

Rationale: There are no industry standards. FSA has adopted the business services standard products based on business need and system requirements.

Oracle Federal Financial System11i will be upgraded to version 11.0.3 this summer (2003).

Mail Server – Microsoft Exchange 2000, Sendmail

Description: FSA uses the Department of Education's mail server for employee email. This is a Microsoft Exchange server that allows FSA employees to access their email through the IMAP standard.

FSA applications that include the ability to send email will use the Sendmail SMTP server. Email services must be coordinated with the VDC personnel and EDNET personnel via FSA CIO VDC operations. The specific machine's IP address that will be generating the email to flow through the Department's Microsoft Exchange resources must be identified, and the SMTP port 25 must be activated on the sending machine in the VDC. If mass mailings (groups of 25 or more messages) are to be sent from any system, this will require extra coordination with the ED CIO personnel. Only outbound mail is processed, no inbound email is allowed to the VDC Servers or devices.

Rationale: Internet Message Access Protocol v4 (IMAP4) permits manipulation of remote message folders, called "mailboxes", in a way that is functionally equivalent to local mailboxes. IMAP4 also provides the capability for an offline client to resynchronize with the server.

Simple Mail Transfer Protocol (SMTP) is an industry standard for sending email. It is described in IETF RFC821.

4.3 Enterprise Data Management

Brief Descriptions

Within FSA, there are two cooperating activities considering data design questions

- Data Architecture
- Data Strategy

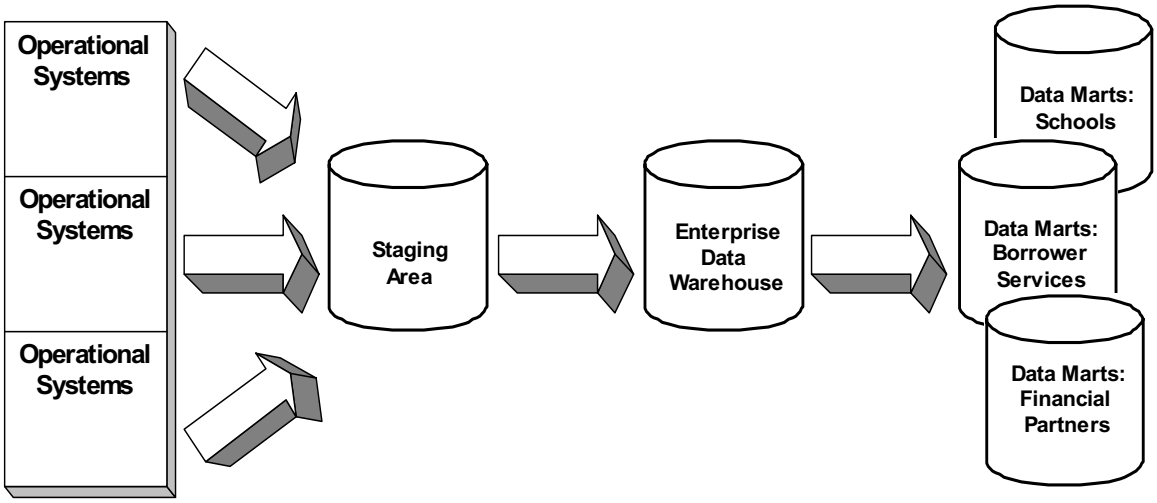
The data architecture group has overall responsibility for the FSA schemes and schema transformations required to improve operations.

The data strategy project is a FY 2003 project to define the various flows among FSA subsystems and to define the data elements that are required for transmission among the subsystems.

Management of data is central to all systems and encompasses the creation, storage, retrieval, use, maintenance, and deletion of data. Enterprise data management services include:

- *Metadata Management* allows data administrators and information engineers to access and modify data about data (i.e., metadata). Metadata can include database schemas, internal and external formats, standard definitions, integrity and security rules, and location within a system. Enterprise data dictionary and repository services also allow end users and applications developers to recommend new data structures or changes to standardized data structures and to obtain logical data structures that will be implemented in the enterprise databases. Data administration functions include procedures, guidelines, and methods for effective data planning, analysis, standards, modeling, configuration management, storage, retrieval, protection, validation, and documentation. The enterprise data dictionary supports data definitions that are used to create data structures in different database management systems (DBMSs).
- *Data Modeling* identifies and clearly defines the entities in which the business must keep data and the important associations between those entities.
- *Database Management Systems (DBMS)* provide controlled access to standardized enterprise data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. DBMS services provide support to different data implementations, including relational, hierarchical, network, object-oriented and flat-file data structures. A relational database management system (RDBMS) is a software system that manages data using the relational model. The relational model conceptually stores data in two-dimensional tables that consist of columns and rows. Tables are related to each other using a primary/foreign key mechanism. Some of the functions performed by the RDBMS are transactional concurrency, backup and recovery, security, enforcement of data integrity, and support for data manipulation. DBMS services are accessible through a programming language interface, an interactive data manipulation language interface such as SQL, or an interactive/fourth-generation language interface.
- *Extract Transform Load (ETL)* services allow the data warehouse data marts and operational data stores to draw data from many different types of operational systems. The elements of the data acquisition services are access to source data, the data warehouse architecture, and end user access. Exhibit 4-1 depicts the flow of data in the data warehouse architecture from the data sources to the data marts.

Exhibit 4-1: Extract Transform Load (ETL)



The source data are the data collected and stored by operational and online transactional processing (OLTP) business applications. Understanding where data is stored across the enterprise is a key component for developing and maintaining data warehouses and data marts. FSA source data will come from the DBMS, legacy systems, enterprise resource planning (ERP) systems, and external sources.

- *Data Warehouse* services provide read-only, time-dependent data for end user access, online analysis, and reporting. This is after extract, transform, and load (ETL) procedures. The data warehouse is the point of integration between the enterprise ETL and the ETL feeding the data marts. The data warehouse architecture encompasses the hardware and software that support the processing, storage, and access of data as it flows from the source to the end user. The major data stores within the FSA data warehouse architecture are:

  Staging—a temporary area in which data is staged for transformation and loading into the data warehouse.

  Data Warehouse—an integrated and centralized data store organized for end user reporting and analytical access.

  Data Marts—subject groupings by business area or data area.

End User Access services provide the mechanisms and architecture to access and display data in an understandable and flexible way to the end user. There are multiple ways to move data from the source to the end users, depending on requirements. Access mechanisms include

query and reporting tools, online analytical processing (OLAP) tools, and data mining and knowledge discovery. With end user access, appropriate security controls must be considered.

- *Imaging* services provide data acquisition through scanning of print documents so they can be archived, searched, and retrieved in electronic format.
- *Enterprise Architecture Management* provides a tool for collecting, integrating, and rendering information about the entire FSA enterprise within the data, business functions, security, networking, people, schedule, and strategy domains.

FEAPMO is scheduled to release the "Data and Information Reference Model". The reader may want to check the FEAPMO website periodically (visit http://www.feapmo.gov).

Target Standards

Target Standards: Enterprise Data Management

	FY 2003	FY 2004	FY 2005
Metadata Management			
	TBD	TBD	TBD
Data Modeling			
Standard Product	Popkin System Architect 8.8.13	Popkin System Architect 9.1	Popkin System Architect 9.1
De Facto Product	Sybase Power Designer 7.0	Sybase Power Designer 7.0	Sybase Power Designer 7.0
De Facto Product	Computer Associates CoolGen 5.1	Computer Associates Advantage:Gen 6.5	Computer Associates Advantage:Gen 6.5
Database Management (Mod System & Data Mart)			
Standard Product	Oracle 8i 8.1.7	Oracle 8i 8.1.7.4	Oracle 9*i*
Standard Product	IBM DB2	IBM DB2	IBM DB2
Extract Transform Load (ETL)			
Standard Product	Informatica Power Center Server 5.2	Informatica Power Center Server 6	Informatica Power Center Server 6
Data Warehousing Technologies			
Standard Product	MicroStrategy 7i	MicroStrategy 8	MicroStrategy 8
Standard Product	MicroStrategy Intelligence Server 7.2	MicroStrategy Intelligence Server 7.2	MicroStrategy Intelligence Server 7.2
Standard Product	MicroStrategy Web 7.2	MicroStrategy Web 7.2	MicroStrategy Web 7.2
Standard Product	Narrowcaster 7.2	Narrowcaster 7.2	Narrowcaster 7.2
Standard Product	MicroStrategy Agent 7.2	MicroStrategy Agent 7.2	MicroStrategy Agent 7.2
Standard Product	Architect 7.2	Architect 7.2	Architect 7.2
Standard Product	Crystal Reports 8.0	Crystal Reports 8.0	Crystal Reports 9.0
Standard Product	WebFOCUS	WebFOCUS	WebFOCUS
Imaging			
Standard Product	Optika Accorde Suite	Optika Accorde Suite	Optika Accorde Suite

De Facto Product	IBM Image Plus	IBM Image Plus	IBM Image Plus
Enterprise Architecture Management			
Standard Product	Popkin System Architect 9.1	Popkin System Architect 9.1	Popkin System Architect 9.1

Approved Standards

Metadata Management – TBD

Description: FSA metadata management will represent an enterprise-wide definition of shared data. FSA's metadata management services will provide the ability to:

- Track traditional metadata, such as file structure definitions, database field names, and lengths and standards found in a data model.
- Manage technical metadata, such as field-to-field mappings between source and target and query response times.
- Store business metadata, such as business rules describing what is and is not included within the data warehouse and definitions of business hierarchies and KPIs.

The metadata management services will include a metadata repository. The metadata repository will contain detailed information on the data warehouse tables, attributes, facts, and relationships. This central data repository will allow for reports to be created once and deployed through the Micro Strategy applications.

Rationale: TBD

Data Modeling – Sybase Power Designer 7.0

Description: Data modeling will support *object-relational* database application design. In addition to automating the design, maintenance, and recovery of back-end relational database applications, data modeling will help FSA design the user-defined data types to be stored in their database, as well as the business logic used to access and manipulate database information. Data modeling technology will allow FSA to import existing information into class diagrams and import a database SQL script into a physical data model, or recover an existing database through an ODBC connection.

Rationale: No published industry standard identified.

Database Management – Oracle 8i 8.1.7, IBM DB2

Description: All new development will be based on relational database management systems.

Rationale: The FSA standard is an object-relational database conforming to the SQL 92 standard. This type of database is a relational database that supports the object operation. FSA will use SQL and some extensions to support the objects; this will provide backward compatibility to previous releases. FSA has selected Oracle 8*i* (mid-tier) and DB2 (mainframe) as its database standards.

Oracle 8i 8.1.7 will be upgraded to 8i 8.1.7.4 this summer (2003).

Extract Transform Load (ETL) – Informatica Power Center Server 5.2

Description: FSA uses an ETL tool with its own global meta-repository and its own server. FSA uses an engine-based approach to access source data, and all data extraction is via the FSA ETL process.

Rationale: The industry has not agreed on a single set of standards for products used to populate a data warehouse. The Informatica Power Center tool populates the FSA data warehouse.

Data Warehousing Technologies – MicroStrategy 7i, Intelligence Server 7.2, Web 7.2, Narrowcaster 7.2, Agent 7.2, Architect 7.2, Crystal Reports 8.0, WebFOCUS

Description: FSA will use MicroStrategy OLAP tools to provide end user access to the enterprise data warehouse and data marts. The following table lists these tools and their functions:

Product	Function
Intelligence Server 7.2	ROLAP report delivery (mid-tier)
Web 7.2	ROLAP analysis over the Web
Narrowcaster 7.2	Report broadcasting
Agent 7.2	Client workstation application
Architect 7.2	Client workstation application
Crystal Reports 8.0	Reports
WebFOCUS	OLAP

Rationale: No published industry standard identified.

Imaging – Optika Accorde Suite, IBM Image Plus

Description: FSA currently has several imaging systems in place. While there is no standard for the manner in which imaging services acquires document data, a standard file format for storage may be established.

Rationale: There is no dominant industry standard for imaging services.

Enterprise Architecture Management – Popkin System Architect 9.1

Description: System Architect serves as a repository for documentation of the enterprise architecture. It also renders depictions of the enterprise architecture and key relationships between FSA data, business functions, security, network, people, schedule, and strategy.

Rationale: There is no dominant industry standard for enterprise architecture management tools. The industry does employ several frameworks for organizing the information within the enterprise architecture. Of these, FSA has adopted a modified Zachman Framework which is also used by the Department of Education.

4.4 Distributed Computing

Brief Descriptions

Distributed computing services are required to operate across physically dispersed applications. New technologies for the internet, distributed objects, and security are accelerating the trend toward distributed computing. The combination of computing platforms and communications networks is the key enabling element for modern information systems. The need to support e-business naturally drives the need to interconnect applications. Networks become increasingly important as organizations migrate to distribute processing.

- *Application Servers* provide a deployment platform and execution environment in which application components can take advantage of application server services, such as security functions and transactions, through a web browser. In this environment, individual applications and application components implement business functions with the services provided by the application server. Most application servers provide thread management,

database connection pooling, persistence, memory management, logging, naming and directory services, security, application management, transaction support, automatic load balancing, and automatic fail-over support.

- *Web Servers* enable organizations to manage and publish information and deploy network-centric applications over the Internet (public) and intranet (private) environments.
- *Web Server Monitoring* provides an analysis of the performance and usage of web servers so that necessary scaling of capabilities or system design can be assessed.
- *Middleware* provides a standard API across hardware and operation system platforms, as well as, networks. Message Oriented Middleware (MOM) performs inter-process messaging that distributes data and control through middleware technology that uses message passing and message queuing to provide peer-to-peer asynchronous communication among programs. Message passing technology has its foundation in a message passing model in which client application programs call an API with as few as four verbs: open connection, send, receive, and close connection. In a distributed message passing model, a client sends a request to the server in the form of a message. The server receives the message and processes the request. The server often creates a new message containing the reply and sends this reply message to the client. Message queuing technology is inherently connectionless. Many message queuing implementations never establish a direct connection between the application client and the application server. With message queuing, however, the sender and receiver can communicate without simultaneous availability, and without the network's direct availability between the sender and receiver. The capability to support discontinuous communication makes message queuing more tolerant of a WAN than other IPC technologies.
- *Application Specific* standards are used in deploying applications throughout the enterprise.

Target Standards

Target Standards: Distributed Computing

	FY 2003	FY 2004	FY 2005
Application Server			
Standard Product	IBM WebSphere Enterprise Edition 3.5.5/5.0*	IBM WebSphere Enterprise Edition 5.0	IBM WebSphere Enterprise Edition 5.0
Standard Product	Oracle Application Server 8.0	Oracle Application Server 9i	Oracle Application Server 9i
Web Server			
Standard Product	IBM IHS Server v1.3.12	IBM IHS Server 1.3.26	IBM IHS Server 1.3.26
De Facto Product	Microsoft IIS 4.0	Microsoft IIS 4.0	Microsoft IIS 4.0

Web Server Monitoring			
Standard Product	WebTrends Enterprise Reporting Server 3.6	WebTrends Enterprise Reporting Server 3.6	WebTrends Enterprise Reporting Server 3.6
Standard Product	SAS	SAS	SAS
Middleware			
Standard Product	IBM MQSeries Server 5.2	IBM MQSeries Server 5.2	IBM MQSeries Server 5.2
Standard Product	IBM MQSeries Client 5.2	IBM MQSeries Client 5.2	IBM MQSeries Client 5.2
Application Specific			
Technical Standard	J2EE Compliant	J2EE Compliant	J2EE Compliant

Approved Standards

Application Servers – IBM WebSphere Enterprise Edition v3.5.5/5.0*, Oracle Application Server 8.0

** Oracle Application Server 8.0 will be updated to Oracle Application Server 9i for FY2004 and FY2005.*

Description: FSA application servers will extend FSA's capabilities by hosting net-centric applications as well as providing application architecture for enabling the development and execution of common services across different business capabilities. The FSA application server will deploy and manage enterprise application components and services; provide secure, web-enabled access to both web-based and legacy application services; and provides an open, standards-based opportunity for reuse of enterprise business logic.

* Applications hosted within the Integrated Technology Architecture (ITA) environment are scheduled to be upgraded from IBM WebSphere Application Server (WAS) 3.5.5 to WAS 5.0 during the months of March through September 2003.

Rationale: The FSA application server will comply with the following standards:

WAS 3.5.5:

- Java Virtual Machine (JVM) compliant with Java v1.2 or greater;
- Support Enterprise Java Beans (EJB) v1.0 or greater;
- Support Java Server Pages (JSP) v1.0 or greater;
- Support Java Servlet API 2.1;
- Support for Java Database Connectivity (JDBC);
- Support for Java Naming and Directory Interface (JNDI);

- Support for Java Messaging Service (JMS) and Java mail standards;
- Support for MIME.

WAS 5.0:

- Java Virtual Machine (JVM) compliant with Java v1.3.1 or greater;
- Support Enterprise Java Beans (EJB) v2.0 or greater;
- Support Java Server Pages (JSP) v1.2 or greater;
- Support Java Servlet API 2.3;
- Support for Java Database Connectivity (JDBC);
- Support for Java Naming and Directory Interface (JNDI);
- Support for Java Messaging Service (JMS) and Java mail standards;
- Support for MIME.

Web Servers – IBM IHS Server v1.3.12, Microsoft IIS 4.0

Description: The FSA web servers will provide client communication, transfer security, dynamic page services, and application logic. This will allow FSA to handle client requests for HTML pages, process scripts such as Java Server Pages (JSP), and cache Web pages.

Rationale: Web server products must support the FSA COE, including platform support and internet protocols (HTTP). The standards are:

- Support HTTP v1.0 and HTTPS
- Support JSP v1.0 or greater
- Support Java Servlet API 2.1
- Support SSL
- FIPS 140-1 compliant

IBM HIS Server version 1.3.12 will be upgraded to version 1.3.26 summer (2003).

Web Server Monitoring – WebTrends Enterprise Reporting Server 3.6, SAS

Description: FSA will monitor web traffic to determine web server performance and usage patterns. This information will be used to drive system upgrades or configuration changes necessary to maximize performance, stability, and availability of HTML content.

Rationale: There is no established industry standard for web server monitoring. Several competing products exist. The FSA standard is based on the specific enterprise requirements identified for web server monitoring.

Middleware – IBM MQSeries Server v5.2, IBM MQSeries Client v5.2

Description: FSA will have an open and scalable messaging and information infrastructure, which will be used to integrate business processes across different hardware and software platforms. This tool will exchange information among applications across several platforms, such as from Mainframes-OS/390 MVS, HP/UX, Sun Solaris, and Windows. FSA will provide an automated solution to integrate software applications across the enterprise, provide rules engine routes for every message to the correct location with table-driven rules bases, and transform data on the fly across DB2 and Oracle application systems.

Rationale: The Message Passing Interface (MPI-2) and the Oxford University Bulk Synchronous Parallel (BSP) model are emerging standards for portable messaging APIs and interoperable messaging protocols. The FSA standard is MPI-2 and BSP.

Application Specific Standards – J2EE

Description: FSA will have an open and scalable messaging and information infrastructure, which will be used to integrate business processes across different hardware and software platforms. This standard will exchange information among applications across several platforms, such as from Mainframes-OS/390 MVS, HP/UX, Sun Solaris, and Windows. FSA will provide an automated solution to integrate software applications across the enterprise, provide rules engine routes for every message to the correct location with table-driven rules bases, and transform data on the fly across DB2 and Oracle application systems.

Rationale: The Java 2 Platform, Enterprise Edition (J2EE) defines the standard for developing multi-tier enterprise applications. J2EE simplifies enterprise applications by basing them on standardized, modular components, by providing a complete set of services to those components, and by handling

many details of application behavior automatically, without complex programming.

4.5 Data Interchange

Brief Description

Data interchange services provide specialized support for the exchange of information between applications and the external environment. These services are designed to handle data interchange between applications on the same platform and applications on different platforms. Data interchange services include:

- *XML Servers* provide secure, high-volume data integration between systems. This allows for structured, application-independent and database-independent data transfer between enterprises over the Internet via encrypted XML-formatted documents.
- *File Transfer* services allow users to copy, replicate, or move whole files across a network.
- *Electronic Data Interchange* (EDI) is the intra- and inter-organizational, computer-to-computer exchange of information in a standard format without human intervention. The idea behind EDI is to take what has been a manually prepared form, a form from a business application, or information, translate that data into a standard electronic format, and transmit it. At the receiving end, the standard format is "untranslated" into a format that can be read by the recipient's application. Hence, output from one application becomes input to another through the computer-to-computer exchange of information. The benefits of EDI are:

  Cost reductions from eliminating paper document handling and faster electronic document transmission.

  Improvements in overall quality through better record keeping, fewer errors in data, reduced processing time, less reliance on human interpretation of data, and minimized unproductive time.

  Better information for management decision-making. EDI provides accurate information and audit trails of transactions, enabling businesses to identify areas offering the greatest potential for efficiency improvement or cost reduction.

  Optimum benefits are achieved through reengineering business processes and utilizing EDI and other electronic commerce technologies as enablers.

- *File Compression* is used to reduce the size of data files being transferred. This results on a lower bandwidth consumption, especially for large data files.

Target Standards

Target Standards: Data Interchange

	FY 2003	FY 2004	FY 2005
XML Server			
De Facto Product	Innovision XML Server	Innovision XML Server	Innovision XML Server
File Transfer			
Technical Standard	FTP, HTTP, SMTP	FTP, HTTP, SMTP	FTP, HTTP, SMTP
Standard Product	CommerceQuest Data Integrator 4.0.1	CommerceQuest Data Integrator 4.0.1	CommerceQuest Data Integrator 4.0.1
De Facto Standard	FTAM and SNA	FTAM and SNA	FTAM and SNA
Electronic Data Interchange			
Technical Standard	XML (May 5 W3C)	XML (May 5 W3C)	XML (May 5 W3C)
Standard Product	bTrade	bTrade	bTrade
File Compression			
Standard Product	Compress	Compress	Compress
Standard Product	WinZip 8.0	WinZip 8.0	WinZip 8.0

Approved Standards

XML Server – Innovision XML Server

Description: The FSA XML server will provide data security services, XML parsing services, and XML processing services. This will allow FSA to send XML-formatted data securely over the Internet using HTTPS encryption; read XML-tagged documents and interpret the self-described data structure of the data elements; and store XML-parsed data and associated structure in memory—using open standards such as Document Object Model (DOM)—for use by application or database.

Rationale: XML server products must support the application of XML throughout the enterprise using FSA-defined security services and provide for Java-based access to DOM-compliant data structures.

File Transfer – FTP, HTTP, CommerceQuest Data Integrator 4.0.1, SMTP (MIME), FTAM, and SNA

Description: FSA standards for file transfer are FTP, HTTP, SMTP, FTAM, and SNA. SMTP will be the FSA standard for mail systems. FSA will select file transfer systems that conform to widely accepted industry standards and promote

interoperability between the defined platforms. The use of e-mail methods for file transfer will be limited to small files and driven by specific business requirements that cannot be met by other standard technologies.

Current tools and methods assume that any encryption requirements are handled before and after file transfers. Future implementations will likely integrate encryption support.

Rationale: The TOG and ISO standards for File Transfer, Access, and Management (FTAM) help provide this service across a heterogeneous network of conforming systems. In addition, File Transfer Protocol (FTP) is an industry-prevalent mechanism that is found with most TCP/IP implementations. Although FTAM and FTP are specialized means of transferring files, it is also possible to use the e-mail system for transporting files. A standard called Multipurpose Internet Mail Extensions (MIME), which has emerged from the Internet mail protocol (SMTP), permits various file types to be transferred as mail attachments. All mail systems have limits on the size of files they can transfer; some are as small as 32 KB.

Electronic Data Interchange – XML, bTrade

Description: FSA will develop new intra- and inter-organizational data interchange using XML or the related W3C standards (e.g., X-Schema, XQL, XLink). FSA will use EDI with XML for continued data distribution with schools, guarantor agencies, and other business partners. Until all systems implement XML, bTrade will also be used. As part of the finance industry, FSA will participate in and adopt data interchange standards generally accepted by partners and customers (e.g., Rosetta-Net).

Rationale: XML is based on the Standard Generalized Markup Language (SGML) from which HTML is also derived. XML allows the inclusion of values of data within a document, such as <price>9.99</price>. XML may be the means to bridge EDI to eCommerce.

bTrade is an application used by the Student Aid Internet Gateway (SAIG) application to transfer all financial data between schools and FSA.

File Compression – Compress, WinZip 8.0

Description: FSA will use file compression on large data files to be transferred over the network. Files will also be compressed when they are archived. File compression standards will be dependent on the capabilities of the operating

system being used.

Rationale: Compress and Zip file compression formats are de facto industry standards and provide compatibility with products available to users external to FSA.

4.6 Network Services

Brief Descriptions

Network services support distributed applications requiring data access and applications interoperating in heterogeneous or homogeneous networked environments. Network services consist of both an interface and an underlying protocol and include the following:

- *Application Directory Services* provide a central data repository that simplifies communication and the sharing of resources. It allows diverse applications, machines, and users (both inside and outside the enterprise) to access the same information and services, which simplifies tasks such as e-mail naming and addressing, maintenance of computing environments, and user authentication and authorization.
- *Transfer Protocols* delivers end-to-end services across physically and logically diverse data networks. Physically diverse networks range from LANs in separate departments to enterprise networks owned by separate companies. Logically diverse networks are defined by the different architectures or products used in their construction.
- *Application Gateways* provide load balancing and redirection of network connections where applicable.
- *Network Address Management Services* provide address translation services from domain names to IP addresses and vice versa.
- *Network Naming Services* require that network administrators provide names for all network resources including printers, users, etc. Advanced directory-services (e.g. LDAP) provide light-weight database access to provide more comprehensive network information.
- *Remote Access* provides secure distributed computing resources into the field. Remote clients have two methods of accessing local enterprise network resources: over the Public Switched Telephone Network (PSTN) or by "tunneling" through the internet. Remote access allows a remote user to dial into a central server and operate exactly as a direct connection to the LAN. Network protocols are transferred transparently across the connection, allowing security and authentication. Remote Node applications scale well, since the connection is largely transparent to the user and multiple calls can be consolidated onto a single ISDN and/or modem server for LAN access.
- *Virtual Private Networks (VPN)* are private, secured networks that exists within a public network and are shared by many private users. Internet-based VPNs replace high-cost wide-

area or enterprise-level networking solutions while providing high-speed access to corporate systems for remote users. Internet VPNs work by creating a tunnel within the public Internet and transmitting encrypted information. Internet VPNs are not optimal as the corporate backbone network, for the transmission of streaming data or multimedia, or when a high level of data security is required. Internet VPNs are well suited for thin-client applications, such as web browsers, e-mail, and other applications that have minimal data transmissions and can tolerate disruptions and delays.

- *Physical Layer* is the type of hardware that comprises the network.
- *Wireless Devices* use wireless network transfer protocols to access FSA services provided over FSA's intranet or the internet.

Target Standards

Target Standards: Network Services

	FY 2003	FY 2004	FY 2005
Application Directory Services			
Technical Standard	LDAP	LDAP	LDAP
Standard Product	Sun One Directory Server	Sun One Directory Server	Sun One Directory Server
Transfer Protocols			
Technical Standard	TCP/IP	TCP/IP	TCP/IP
Technical Standard	SNA	SNA	SNA
Application Gateway			
Standard Product	Computer Associates Java Proxy	Computer Associates Java Proxy	Computer Associates Java Proxy
Standard Product	Computer Associates COMM Proxy	Computer Associates COMM Proxy	Computer Associates COMM Proxy
Network Address Management			
Technical Standard	DHCP	DHCP	DHCP
Technical Standard	Static IP	Static IP	Static IP
Technical Standard	NAT	NAT	NAT
Network Naming Services			
Technical Standard	DNS	DNS	DNS
Remote Access Services			
Standard Product	Cisco Secure RADIUS	Cisco Secure RADIUS	Cisco Secure RADIUS
Standard Product	Citrix	Citrix	Citrix
Virtual Private Network			
Standard Product	CheckPoint VPN-1	CheckPoint VPN-1	CheckPoint VPN-1
Physical Layer			
Technical Standard	Ethernet	Ethernet	Ethernet
Wireless Devices			
Standard Product	Blackberry 2.1	Blackberry 2.1	Blackberry 2.1

Approved Standards

Application Directory Services – Sun One Directory Server (formerly Netscape Iplanet), LDAP

Description: The FSA directory server will provide name and domain services, including single sign-on capability, common data store for personalization preferences, and common source of user authentication and privileges.

Rationale: LDAP (Lightweight Directory Access Protocol) is an industry standard for directory services.

Transport protocols – TCP/IP

Description: FSA is committed to migrating to a single managed, secure, wide area data network. FSA will migrate to the TCP/IP network protocol and increasingly restrict the use of SNA traffic.

When new system applications are connected to the internet, specific ports must be activated for services to gain access. Typically, the following ports are opened in a development environment:

- FTP ports 20/tcp & 21/tcp
- Telnet port 23/tcp
- WWW port 80
- SSL port 443

Other ports may be required to access a certain application software services and the FSA VDC operations staff must open each end.

There are a series of "security hole" ports that will not be opened to either the internet or through the private connection to EDNET. They are:

- Microsoft Net bios ports 137, 138, 139 ; netbios-ns -137/tcp, netbios-ns - 137/udp, netbios-dgm -138/udp, netbios-ssn - 139/tcp
- SNMP ports 161/udp & 162/udp
- Instant Messenger ports

As a general rule UDP ports are not activated and ICMP is shut down, except for specific troubleshooting instances.

Rationale: TCP/IP is a strategic step toward interoperability. It uses a common network infrastructure. TCP is the transport (OSI Level 4) layer, and IP is the network (OSI Level 3) layer.

Application Gateway – Computer Associates Java Proxy, Computer Associates COMM Proxy

Description: COMM and Java Proxies act as gateways, performing Layer 1 to 3 translation for differing protocol stacks, enabling any application to communicate over any transport network. As such, they provide appropriate compensations for functional mismatches between peer layers of different protocols.

COMM Proxy is specific to the Microsoft architectures and Java Proxy to the Java architectures.

Rationale: There is no network standard.

Network Address Management – Dynamic Host Configuration Protocol (DHCP), Static IP, NAT

Description: FSA employs DHCP, which is currently administered by the Department of Education, as its standard network address management service. An assessment of the Infrastructure Architecture will determine if FSA's current DHCP implementation will scale to support native TCP/IP on all desktops. While DHCP is not intended to support mobile users, it is valuable in supporting laptop plug-in at remote locations. DHCP assigns an IP address to the client system, so the DNS database must change before full service catches up.

A static IP address is assigned to servers and specialized development computers only as required.

Rationale: DHCP is an industry standard and is defined in IETF RFC 2200.

Network Naming Services

Description: FSA will utilize a consistent, globally unique naming and addressing scheme. This naming scheme is required for the objects being stored in both naming and directory systems. The names of the objects will be logical and meaningful to the system users and other applications. A name should conform to the following three principles:

- Alphanumeric format that clearly conveys the built-in meaning

- Unique within its domain
- Not overly encoded or in hexadecimal format, except for security purposes

Rationale: The FSA standard for naming services is DNS. Currently, DNS services are administered by the Department of Education. ED CIO personnel make all DNS entries, as they are responsible for maintaining the "ed.gov" domain services. The FSA Web Master can make some internal only DNS entries. No DNS services are available at the VDC. DNS change requests are submitted via the CCRB process. The System Change Request (SCR) is online at http://tested/ccrb.shtml (for those on EDNet).

FSA will consider implementing an integrated, hierarchical directory service (e.g. Sun One LDAP) based on the LDAP and X.500 directory services standards in the next iteration of the infrastructure architecture. X.500 is the leading standard for directory services. The X.509 standard (the ITU-recommended standard for digital certificates) should be fully supported in any selection of an X.500 directory system.

Remote Access –Cisco Secure RADIUS, Citrix

Description: The FSA standard will be PPP, which will be used for connecting to networks over standard serial (telephone) lines.

Rationale: Using a modem to connect to a terminal server, with point-to-point protocol (PPP) there is a more direct and flexible connection. Many of the functions accessed by dialing up a terminal server and running them on a remote host (such as a UNIX shell account) can also be run from a personal computer. For instance, PPP allows the use of e-mail and web browser programs that take advantage of a workstation's graphics capabilities, graphical user interface, and other special features.

Virtual Private Network – CheckPoint VPN-1

Description: FSA will use VPN software capable of encrypting data for tunneling through network connections through the public internet. Checkpoint VPN-1 is the VPN client used to access the FSA network. A subcomponent of the Checkpoint Firewall is the server side of this service.

Rationale: IPSec (IP Security Protocol) is an IETF standard for the encryption of data transport through the IP network layer.

Physical Layer – Ethernet

Description: Ethernet is the principle network physical layer standard for FSA.

Rationale: Ethernet is a recognized industry standard for network physical layer.

Wireless Devices – Blackberry 2.1

Description: FSA will employ wireless devices that extend network services to allow mobility while maintaining the ability to access information and communicate with others. The wireless devices will conform to current FSA network services standards when applicable.

Rationale: The Blackberry device allows access to organization email, web pages, and text messaging while not requiring new network services to be employed.

4.7 Operating Systems

Brief Description

Operating system services are responsible for the management of platform resources, including the processor, memory, files, and input and output. They generally shield applications from the implementation details of the machine. Operating system services include:

Kernel operations, which provide low-level services necessary to create and manage processes and threads of execution, execute programs, define and communicate asynchronous events, define and process system clock operations, implement security features, manage files and directories, and control input/output processing to and from peripheral devices.

Command interpreter and utility services, which include mechanisms for services at the operator level, such as comparing, printing, and displaying file contents, editing files, searching patterns, evaluating expressions, logging messages, moving files between directories, sorting data, executing command scripts, local print spooling, scheduling signal execution processes, and accessing environment information.

Batch processing services, which support the capability to queue work (jobs) and manage the sequencing of processing based on job control commands and lists of data.

File and directory synchronization services, which allow local and remote copies of files and directories to be made identical. Synchronization services are usually used to update files after periods of off line working on a portable system.

The operating system platforms employed by FSA provide the following capabilities:

- *Mainframe (Tier 1) Hosts/Servers* operating system provides one host that communicates with multiple clients. Users can explore existing corporate data to locate patterns and structures that will provide answers to real-world business questions or new business opportunities. A system with DB2 will provide the capability for handling large databases as a single image.
- *Mid-Tier* operating system services provide the basic environment for running applications. (See the discussion on personal computer operating systems.)
- *Personal Computer (Tier 3)* operating systems using Intel's microprocessors running Microsoft Windows NT and 2000 Workstation are also being used in high-end computing applications such as application development, multimedia, and decision support data analysis presentation. NT Workstation offers the same user interface and similar user services as Windows, which is more commonly used in general office automation environments today. Both of these operating systems can run on the same hardware platforms, enhancing the ability to combine the right operating system technology with the correct price and performance hardware technology to deliver high-function personal computing to end users. This approach allows performance upgrades to be accomplished more easily during the end user application life cycle.
- *Mobile Devices* operating system services provide some of the same capabilities as the Personal Computer operating system for use on a mobile device. Typically, mobile devices will use applications that provide a scaled down set of capabilities.

Target Standards

Target Standards: Operating Systems

	FY 2003	FY 2004	FY 2005
Mainframe (Tier 1) Hosts/Servers			
Standard Product	OS/390 MVS v2.11		
Standard Product		ZOS	ZOS
Standard Product	CICS	CICS	CICS
Mid Tier (Tier 2) Servers			
Standard Product	HP/UX 11i	HP/UX v11i	HP/UX v11i
Standard Product	HP/UX 10.20	HP/UX 10.20	HP/UX 10.20
Standard Product	Microsoft Windows NT 4.0		
Standard Product	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows .Net
Standard Product	Sun Solaris 8	Sun Solaris 8	Sun Solaris 9

Personal Computers (Tier 3)			
Standard Product	Microsoft Windows 2000	Microsoft Windows 2000	Microsoft Windows 2000
Mobile Devices			
De Facto	Palm OS 4.0	Palm OS 4.0	Palm OS 4.0
Standard Product	Blackberry 2.1	Blackberry 2.1	Blackberry 2.1

Approved Standards

Mainframe (Tier 1) Hosts/Servers – OS/390 MVS v2.11, ZOS (formerly OS/390 MVS), CICS

Description: The operating system will provide an environment for data warehousing, data mining, and decision support applications. The host/server operating system will support current legacy mainframe applications and newly selected COTS applications. The FSA standard for the mainframe operating system is the OS/390 MVS configuration. This OS/390 MVS operating system currently resides on all FSA mainframe systems. FSA uses Parallel Sysplex technology configuration. ZOS will replace OS/390 MVS with version 3.0.

Rationale: FSA will use large-scale servers and enterprise computers with operating systems and hardware components that comply with IEEE's POSIX and Unix95 specifications.

Mid-Tier (Tier 2) Servers – HP/UX v11i, HP/UX 10.20, Microsoft Windows NT v4.0, Microsoft Windows 2000, Sun Solaris 8

Description: The mid-tier operating systems are function-specific providing the functions indicated below:

Target Operating System	Function
Microsoft Windows NT/2000	Application Services Database Services End User Data Access
HP/UX	Oracle Platforms Oracle Federal Financial System Internet Information Technology Architecture
Sun Solaris	Information Technology Architecture

Rationale: Compliance with XPG 4.2 and POSIX standards allows for increased interoperability of hardware components and facilitates application portability. The ability to upgrade processor performance or to add additional processors, disk storage, and communications support extends the life of the platform and enhances the return on investment. ITA is primarily deployed on Solaris and HP/UX platforms.

Personal Computers (Tier 3) – Microsoft Windows 2000

Description: The operating system must ensure compatibility and the sharing of data with other personal computer operating systems within FSA's environment and comply with POSIX standard interfaces for long-term usability. FSA has committed to the Microsoft Office and MS Outlook Windows operating system family as a means to establishing a common desktop environment.

Rationale: The personal computer operating system will comply with the FSA Desktop COE and support FSA's standard set of productivity tools. The FSA standard product selection is Microsoft Office 2000 and Windows 2000.

Mobile Devices – PalmOS 4.0 / Blackberry 2.1

Description: These mobile device operating systems will provide basic capabilities that enhance the FSA business process while allowing user mobility. Currently, there is no FSA standard, but PalmOS, Blackberry and Windows CD are emerging as front-runners in the industry.

Rationale: FSA has not adopted a standard product mobile device operating system as these devices have not become part of the core business tools used by the organization

4.8 Application Development

Brief Description

Software development for FSA applications will utilize a variety of tools, processes, and methodologies. Standards for these are given in the *FSA Software Engineering Guide* (visit http://fsanet.ed.gov/cio/techcenter/technology_handbook/1/newtoc.pdf , section 4).

There are several different stages of application development. Each stage has a corresponding set of tools. These include the following services:

- *Application Design* tools are used to model the conceptual model of an application. This will include descriptions of objects, classes, methods, and interobject communication.
- *Programming Tools* are used to create, edit, debug, and compile computer code.
- *Application Testing* tools are used to prepare a component test model, establish a component test environment, and execute a component test.
- *Code Management* tools serve as repository for computer code. They allow the control of versions, merging of multiple forks of code, and check-in and check-out of code that is being edited.

Target Standards

Target Standards: Application Development

	FY 2003	FY 2004	FY 2005
Application Design			
Standard Product	Rational Rose 2002	Rational Rose 2002	Rational Rose 2002
Programming Tools			
Standard Product	IBM WebSphere Studio Application Developer (WSAD) 5.0	IBM WebSphere Studio Application Developer (WSAD) 5.0	IBM WebSphere Studio Application Developer (WSAD) 5.0
Standard Product	Sun Java Development Kit 1.3	Sun Java Development Kit 1.3	Sun Java Development Kit 1.3
Standard Product	Oracle JDeveloper	Oracle JDeveloper	Oracle JDeveloper
De Facto Product	Computer Associates CoolGen 5.1		
Application Testing			
Standard Product	Mercury Interactive Loadrunner	Mercury Loadrunner 7.5	Mercury Loadrunner 8
Standard Product	Rational TestManager	Rational TestManager	Rational TestManager
Code Management			
Standard Product	Rational ClearCase 2002	Rational ClearCase 2003	Rational ClearCase 2003
Standard Product	Rational ClearQuest 2002	Rational ClearQuest 2003	Rational ClearQuest 2004
De Facto Product	Computer Associates Harvester Change Manager	Computer Associates Harvester Change Manager	Computer Associates Harvester Change Manager
De Facto Product	Computer Associates Endeavor	Computer Associates Endeavor	Computer Associates Endeavor

Approved Standards

Application Design – UML-Style Diagrams (PowerDesigner, Rational Rose, Visio, etc.)

Description: FSA will use tools that are capable of producing Unified Modeling Language (UML)-Style diagrams plus schemas and/or code as appropriate.

Rationale: While technically a collection of diagramming techniques rather than a language, UML is a widely accepted technique for depicting data modeling artifacts. Several widely used COTS tools will generate the diagrams and/or schemas and code as appropriate. Some will also reverse-engineer existing schemas into the UML diagram format.

Programming Tools – IBM WebSphere Studio Application Developer (WSAD) 5.0, Sun Java Development Kit 1.3,Oracle JDeveloper, Computer Associates 5.1CoolGen

Description: FSA will use a programming tool that is capable of developing J2EE compliant applications.

Rationale: J2EE is an industry standard set of interobject communication protocols.

Application Testing – Mercury Interactive Loadrunner, Rational TestManager

Description: FSA uses the listed tools for testing applications. All testing is done outside of the network firewall.

Rationale: No predominant industry standards exist.

Code Management – Rational ClearCase 2002 (Non-Mainframe), Rational ClearQuest 2002 (Mid-Tier), Computer Associates Harvester Change Manager (Mid-Tier), Computer Associates Endeavor (Mainframe)

Description: FSA will use code management tools capable of merging multiple development branches and of checking in and checking out code for editing.

Rationale: No predominant industry standards exist.

4.9 Systems Management

Brief Descriptions

Systems management refers to information technology activities that do not relate to application execution or development. It includes everything from the daily operations, management, and service of information system to long-range planning for future business needs. Systems management comprises the processes, procedures, tools, and techniques that are implemented through personnel and automation to ensure the cost-effective operation of information systems. The procedures and tools ensure proper planning, configuration, and problem handling of IT resources. Systems management includes the following:

- *Configuration Management (CM)* enables maintaining, adding, and updating the relationships among components and the status of components themselves during system/network operation. End user service is provided by the configuration of the various system and network components into an integrated and cohesive function. CM includes the automatic capture and storage of program component relationships and maintenance of the history of those relationships and transformations. It is becoming increasingly difficult to maintain, control, and manage software. CM addresses all aspects of managing software and its changes with complete security, integrity, and audit capability for the life of the software. CM includes both version control and release management.
- *Inventory Management* provides a repository of accurate and timely data about managed resources. Inventories are used to track expected occurrences of the resources against the actual existence of the resources. Inventories may also include various reference information such as location, owner, or vendor contact.
- *Operations Management* supports and controls the current, implemented infrastructure. The primary tasks of operations include the following:

  Fault management—Fault identification, isolation, recovery, resolution, and message filtering.

  Performance management—System and network data collection and logging through monitoring and controlling. Monitoring tracks activities on the system/network. Controlling enables performance management to make adjustments to improve system/network performance.

  Change control—Change coordination, approval, and implementation.

  Accounting management activities—Ability to determine by cost centers, or even individual project accounts, the use of systems/network services. Additionally, the systems/network manager needs the ability to track the use of system/network resources by component or component class (type).

Hierarchical storage management—Dynamic placement of data across various storage technologies such as memory, disks, and tapes, based on usage and retention parameters.

Routine activities—Scheduling and common services such as backups and preventive maintenance.

- *Load Balancing* has three major components. (1) Load balancing software, which distributes web site traffic between servers, leading to better response times for online users. (2) Caching proxy server, which captures web site images that can be retrieved locally in subsequent requests, reducing network traffic. (3) Enterprise file system, which provides content replication.
- *Network Inventory and Distribution Services* provide a mechanism for centrally distributing and modifying software across distributed environments. For inventory, the system automatically scans for and collects hardware and software configuration information from computer systems in the enterprise.
- *Capability Maturity Model (CMM)* is a model for judging the maturity of the software processes of an organization and for identifying the key practices that are required to increase the maturity of these processes. It is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. The CMM is organized into five maturity levels: Initial, Repeatable, Defined, Managed, and Optimizing. For more information about CMM, visit www.sei.cmu.edu.

Target Standards

Target Standards: System Management

	FY 2003	FY 2004	FY 2005
Configuration Management			
Standard Product	Rational ClearCase 2002	Rational ClearCase 2003	Rational ClearCase 2003
Standard Product	Rational ClearQuest 2002	Rational ClearQuest 2003	Rational ClearQuest 2004
De Facto Product	Computer Associates Harvester Change Manager	Computer Associates Harvester Change Manager	Computer Associates Harvester Change Manager
De Facto Product	Computer Associates Endeavor	Computer Associates Endeavor	Computer Associates Endeavor
Inventory Management			
De Facto	Custom solution	Custom solution	Custom solution

Operations Management			
Standard Product	Computer Associates CA-7 (Mainframe)	Computer Associates CA-7 (Mainframe)	Computer Associates CA-7 (Mainframe)
Standard Product	BMC Control D 3.5 (Printing)	BMC Control D 3.5 (Printing)	BMC Control D 3.5 (Printing)
Standard Product	BMC Control M/R (Mainframe/Mid-Tier)	BMC Control M/R (Mainframe/Mid-Tier)	BMC Control M/R (Mainframe/Mid-Tier)
Standard Product	HP OpenView 3.5 (Network Monitor)	HP OpenView 3.5 (Network Monitor)	HP OpenView 3.5 (Network Monitor)
Standard Product	Computer Associates UniCenter TNG 2.4 (Mid Tier)	Computer Associates UniCenter TNG 2.4 (Mid Tier)	Computer Associates UniCenter TNG 2.4 (Mid Tier)
Load Balancing			
Standard Product	IBM Network Dispatcher 4.0	IBM Network Dispatcher 4	
Standard Product	Cisco Local Director	Cisco CSS	Cisco CSS
Standard Product	HP Service Guard	HP Service Guard	HP Service Guard
Network Inventory and Distribution Services			
Standard Product	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)	Microsoft Software Management System (SMS)
Standard Product	Candle Management	Candle Management	Candle Management
De Facto Product	Lotus Notes	Lotus Notes	Lotus Notes
Capability Maturity Model (CMM)			
IT Organizational Approach	See Website at www.sei.cmu.edu	See Website at www.sei.cmu.edu	See Website at www.sei.cmu.edu

Approved Standards

Configuration Management – Rational ClearCase 2002, Rational ClearQuest 2002, Computer Associates Harvest Change Manager, Computer Associates Endeavor

Description: FSA implements it Enterprise Configuration Management process through the Rational ClearCase and ClearQuest products.

Rationale: No published industry standard ECM identified.

Inventory Management – Custom solutions

Description: Solutions developed by both the Department of Education and FSA are currently being used. FSA will maintain an accurate inventory of the major systems based on the 1997 lawsuit Public Citizen v. Raines.

Rationale: To be determined.

Operations Management – Computer Associates CA-7, BMC Control D 3.5 (Printing), BMC Control M/R, HP OpenView 3.5 (Network Monitor), Computer Associates UniCenter TNG 2.4

Description: FSA will use operations management solutions that ensure individual distributed systems and mainframe technologies effectively create an automated environment.

CSC monitors every device within the VDC through their Global Management facility.

Rationale: The FSA standard will be SNMP (Simple Network Management Protocol) as a generic network management tool. An SNMP message is sent to and from a device to gather information or configure the device.

Load Balancing – IBM Network Dispatcher, Cisco Local Director v3.0, HP Service Guard

Description: Load balancing will provide the following features:

- Rules-based routing to detect and react to sudden increases in activity
- Load balancing based on the content of HTTP requests at an application level
- Use of a public key/private key pair to control communication and make remote administration more secure
- Transparent load balancing and a mechanism to catch and log misdirected or malicious packets
- Proxy sharing of cached content
- Garbage collection based on user-defined usage specifications or at user-specified times
- Remote administration using the security features provided by SSL
- Reverse proxy to permit more concurrent connections and to accelerate Web server performance

Rationale: No published industry standard identified.

Network Inventory and Distribution Services – Microsoft Software Management System (SMS), Lotus Notes, Candle Management

Description: To be determined

Rationale: No published industry standard identified.

4.10 Security Services

Brief Description

The *Office of Management and Budget (OMB) Circular A-130 Appendix III* recommends all federal government agencies implement and maintain a security program that provides "adequate security" for information, processes, and systems. Adequate security is defined as security controls commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information stored or flowing through these systems. Security controls may be physical, management, personnel, operational, or technical, and implemented by hardware or software security.

The *FSA Information Technology Security and Privacy Policy* document provides a view of the existing Department of Education Information Security Policy and how it relates to FSA. It also outlines procedures that should be used to reduce risk and ensure that FSA systems are available to FSA customer and partners. Other security guidance is available in National Institute of Standards and Technology publications.

The *Security Architecture* and *FSA Information Security General Minimum Security Baseline Standards* security documents are current under development by FSA Systems Enhancement Partners. These documents will detail security architecture and standards for FSA. A Minimum Security Baseline (MSB) will be used as the standard for implementing a minimum level of security on all FSA information systems. The following section outlines several technical security policy and standards that should be used to protect FSA information systems, data, networks, and applications.

- *Digital Certificate Servers* provide a specially coded object that uniquely identifies a site. This object contains the site's public key for encryption and the site's identification information. It allows verification of the claim that a specific public key does, in fact, belong to a specific individual. These certificates are used browsers and firewalls to permit or restrict users from accessing or downloading components. Certificate management and access

provide primary components of information security, including authentication, authorization, encryption, and non-repudiation.

- *Firewall Services* protect sensitive information and resources that are attached to a network from unauthorized access. A firewall is a system that prevents the hazards of the internet from extending to internal network. It enforces a boundary between two or more networks. Firewall policies either deny any service (or packet) not explicitly permitted or permit any service (or packet) not explicitly denied. In general the various firewall security mechanisms address themselves to specific layers in the OSI 7-level network model. Several mechanisms can be combined into a comprehensive firewall system, but the mechanisms should be chosen and coordinated so that they do not interfere with each other. A variety of firewall implementations may be required at various levels within the network. Firewalls should encompass both packet filters and proxy services. Packet filters provide network-level security. These are protocol-based services that check the address portion of data packets to determine the desired destination and intent. Administrators can block certain combinations that are categorized as unauthorized. Proxy services provide application-level security. Proxy services shield or screen the server address, thus preventing outsiders from knowing the specific addresses of servers within the private network (and later targeting them).
- *Access Control* is achieved by a combination of physical and logical access. Logical access control permits access to a machine, a file, or an application only after the client (e.g., employee, machine, application) is authenticated.
- *Directory Access Services* provides access control to specific file system locations.
- *Audit Trails Creation* is used to detect penetration of a computer system and reveal usage that identifies misuse. Audit trails may be limited to specific events or may encompass all the activities on a system. Audit trails are maintained but are not used unless needed. As a support for operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. The audit trails have four important security objectives:

  Individual accountability

  Reconstruction of events

  Intrusion detection

  Problem analysis

- *Authentication* is the means of proving the identity of a subject to system, networks, and applications. Entering an assigned value (USERID) performs identification and authentication is performed by entering a value or by physical means. The authentication methods should be totally under the control of the individual. The mechanism for authentication of a user generally depends on one or more of the following: something the user knows (a password or encryption key), something the user possesses (a key, token, or magnetic security badge), or

some physical characteristic (biometrics) of the user such as a fingerprint. Authentication mechanisms employing tokens or biometrics provide a significantly higher level of security than passwords and are referred to as advanced or strong authentication mechanisms. However, when sending information over remote network connections, particularly over public networks without security procedures, it is possible to impersonate users and other entities in a public network.

- *Database Security Services* contribute to the protection of information, data, and resources in open systems in accordance with applicable FSA information domain and information system security policies. An information domain is a set of users, their information objects, and a security policy. An information domain security policy is the statement of the criteria for membership in an information domain and the required protection of the information objects. These information domains are not bounded by systems or networks of systems. The provision of DBMS security services includes the following activities:

  Data security policy management

  Data security service management

  Data security mechanism management

  Data security mechanism support management

- *Electronic Signatures/Non-repudiation* provides the means to prove that a digital transaction actually occurred, i.e., some form of electronic receipt. Digital signatures and file integrity checks use strong encryption to protect data integrity and guarantee data authenticity with a reasonable degree of assurance. FSA may have a need for strong non-repudiation requirements so those individuals can be held accountable for messages they send.
- *Host Intrusion Detection* focuses on events occurring within a system as reported by the various logs in a system, for example, repeated failed logins, attempts to access or modify certain files, or changes in usage patterns. Firewalls will reduce but not entirely eliminate the risk of unauthorized external access to FSA networks and systems. Intrusion detection systems, the digital equivalent of burglar alarms, and alarm messages they produce may be linked into the systems management process.
- *Network Intrusion Detection* focuses on examining packets on the network for known attack patterns. The detection agent functions by looking for actual attempts to exploit the vulnerabilities of the systems and the networks.
- *Physical Security* is an effective means to provide security within individual sites in the FSA computer network. While not practical for security of small remote sites and mobile computers (e.g., laptops), physically restricting access to machines in central locations under FSA control is an important part of overall systems security. Physical security policies may be enhanced through the deployment of appropriate monitoring systems.
- *Encryption* provides protection of information stored and routed on computer networks and contributes to meeting data privacy and integrity requirements. When data is transmitted it must be protected against interception or alteration. Transmission that may need to be

encrypted include remote terminal access, bulk transfer of data extracted from legacy systems and online database access. Firewalls alone cannot protect such data when it is transmitted outside the FSA managed network.

- *Virus Protection* provides virus prevention and detection in a variety of network environments. Many forms of computer information can contain harmful content including viruses, macro viruses, and Trojan horse programs. These "malicious programs" can be transmitted across a network in a number of ways including SMTP e-mail attachments, FTP file downloads, and Java applets. Incoming data can be checked for harmful content at the public Internet work boundary. Passive virus protection should be implemented throughout the network environment. Products chosen should protect against the widest possible array of viruses, and should be compatible with the FSA's architectures.

Target Standards

Target Standards: Security Services

	FY 2003	FY 2004	FY 2005
Digital Certificate Server Services			
De Facto Product	Netscape Certificate Server	Netscape Certificate Server	Netscape Certificate Server
Firewall Services			
Standard Product	CheckPoint Firewall-1	CheckPoint Firewall-1	CheckPoint Firewall-1
Access Control			
Standard Product	IBM RACF (Mainframe)	IBM RACF (Mainframe)	IBM RACF (Mainframe)
De Facto Product	BMC Control SA	BMC Control SA	BMC Control SA
De Facto Product	Computer Associates UniCenter TNG 2.4	Computer Associates UniCenterTNG 2.4	Computer Associates UniCenterTNG 2.4
Directory Access Services			
Technical Standard	LDAP	LDAP	LDAP
Audit Trail Creation			
Technical Standard	System Log File	System Log File	System Log File
Authentication			
Standard Product	IBM RACF (Mainframe)	IBM RACF (Mainframe)	IBM RACF (Mainframe)
Standard Product	Computer Associates UniCenter TNG 2.4	Computer Associates UniCenter TNG 2.4	Computer Associates UniCenter TNG 2.4
Standard Product	Oracle 8i 8.1.7	Oracle 8i 8.1.7.4	Oracle 9i
Standard Product	FSA PIN (Custom Application)	FSA PIN (Custom Application)	FSA PIN (Custom Application)
De Facto Product	BMC Control SA (Mainframe/Mid-Tier)	BMC Control SA (Mainframe/Mid-Tier)	BMC Control SA (Mainframe/Mid-Tier)
Standard Product		Single Sign On (TBD)	Single Sign On (TBD)
Database Security Services			
Standard Product	IBM RACF (Mainframe)	IBM RACF (Mainframe)	IBM RACF (Mainframe)
Standard Product	Oracle 8i 8.1.7	Oracle 8i 8.1.7	Oracle 8i 8.1.7

De Facto Product	Top Secret (Mainframe)		
Electronic Signatures/Non-repudiation			
	TBD	TBD	TBD
Host Intrusion Detection			
Standard Product	Tripwire 2.4.2	Tripwire 2.4.2	Tripwire 2.4.2
Network Intrusion Detection			
Standard Product	RealSecure/Checkpoint	RealSecure/Checkpoint	RealSecure/Checkpoint
Physical Security			
	See OMB A130	See OMB A130	See OMB A130
Encryption			
Technical Standard	Router Encryption (DES3)	Router/Hardware Encryption	Router/Hardware Encryption
Technical Standard	Secure Socket Layer (128-bit)	Secure Socket Layer (128-bit)	Secure Socket Layer (128-bit)
Technical Standard	IPSec	IPSec	IPSec
Standard Product	Verisign (SSL)	Verisign (SSL)	Verisign (SSL)
Standard Product	RSA Bsafe	RSA Bsafe	RSA Bsafe
Standard Product	RSA Bsafe Libraries	RSA Bsafe Libraries	RSA Bsafe Libraries
De Facto Product	Sterling Commerce Connect Direct (used for transactions with the Dept. of Treasury)	Sterling Commerce Connect Direct (used for transactions with the Dept. of Treasury)	Sterling Commerce Connect Direct (used for transactions with the Dept. of Treasury)
Virus Protection			
Standard Product	McAfee VirusScan	McAfee VirusScan	McAfee VirusScan
Standard Product	Norton Enterprise Antivirus 7.1	Norton Enterprise Antivirus 2000	Norton Enterprise Antivirus 2000

Approved Standards

Digital Certificate Server Services – Netscape Certificate Server

Description: The FSA digital certificate server will provide authentication, issuance, and revocation services, including the capability for future digital signature administration. Digital certificate server services will be part of the overall, comprehensive FSA security procedures.

FSA digital certificate server services will be capable of handling large numbers of certificates and will work across all browsers and servers. Authentication services will verify that the presenter of a set of credentials matches the owner on record. Issuance services will generate public/private keypairs. Revocation services will maintain a list of certificates that have been revoked and be able to share that list with other certificate servers.

Rationale: The X.509 digital certificate involves the ITU-T Recommendation X.509 [CCI88c], which specifies the authentication service for X.500 directories as well as the widely adopted X.509 certificate syntax.

Firewall Services – CheckPoint Firewall-1

Description: All communication between the FSA enterprise private network and the public network will pass through the FSA network firewall. The design philosophy of FSA's internet connectivity is to provide unrestricted outbound access to Internet resources with inbound access limited by the firewall rules. This philosophy provides the maximum protection for servers/workstations inside EDNet while allowing EDNet users sufficient access to internet resources.

FSA firewalls will provide policy-driven restrictions on network connections, protocols, and data formats, including authentication-driven restrictions on data exchanges by applications and individuals. This will include the use of a hybrid firewall, which will provide both network-level and application-level security, located between the back-end servers and the certificate server.

The following firewall directives will apply to all existing and future firewall implementations:

- All interconnections to the FSA private intranet from other networks must use the TCP/IP protocol. All protocols/services not specifically noted in this document are prohibited except by specific approval from FSA.
- All existing and future untrusted networks connecting to the FSA private intranet require an FSA-certified firewall implementation.
- Only FSA Security-approved personnel are permitted to perform any firewall administration.
- All firewall interconnections to the FSA private intranet, whether existing or proposed, must be documented and the documentation must be provided to FSA Security.

Rationale: ICSA standards body and relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

Access Control – RACF (Mainframe), BMC Control SA, Computer Associates TNG

Description: Access authorization will be based on the responsibilities and functions performed by the user. This includes application and individual system access. Security profiles will be defined with specific access requirements and will

contain sufficient information to determine which networks, systems, applications and files the user is permitted to access. Access control mechanisms will manage the access attributes of subjects to objects. Only an authorized person will have the ability to grant access to an object.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

Directory Access Services – LDAP

LDAP is discussed in section 4.6: Network Services.

Audit Trail Creation – System Log File

Description: Audit logs are continually appended with system activity. When a security event occurs, the logs are examined to determine the nature of the event. Logs are kept on tape long enough to satisfy the security requirements of the system. Typically, the log files are on disk for 30 days and then archived to tape. These tapes are usually retained for up to 90 days or longer if required.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

Authentication – RACF (Mainframe) BMC Control SA (Mainframe/Mid-Tier), CA UniCenter TNG 2.4 (Mid-tier), FSA PIN (Custom Application), Oracle, Single Sign On (TBD)

Description: Authentication will ensure that every subject or object using the system is identified. Identification will be enforced for login sessions through direct connected devices such as desktop workstations and through remote devices, such as dial-up connections. Typically, an operating system's password authentication capabilities will be used. Other authentication devices such as smart cards, biometrics-measuring devices (fingerprints or retina image) are challenge response methods. No authentication data will be available to unauthorized subjects or objects. Authentication information such as password will never be stored in clear text.

FSA authentication will also encompass the following areas:

- Warning to unauthorized user that the system is security aware
- Authentication of the user

- Password will be at least eight characters long with digits and alpha characters. It must also include at least one capital letter.
- Periodic changing of password
- No reuse of previous three passwords
- Time out of session when left unattended
- Information displayed on entry, about previous successful and unsuccessful login attempts
- Authentication attempt is suspended after three fail attempts

FSA is investigating the implementation of a Single Sign On authentication mechanism that would allow users to have one USERID and password for multiple systems.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

Database Security Services – RACF (Mainframe), Top Secret (Mainframe), Oracle 8i (Mid-Tier)

Description: The database maintains the user, user groups and controls permissions for all database resources – tables, views, fields, and other database objects. Most databases have their own list of users and groups.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

Electronic Signatures/Non-repudiation – TBD

Description: To be determined.

Rationale: To be determined.

Host Intrusion Detection – Tripwire 2.4.2

Description: FSA host intrusion detection will be widely deployed and will be a trusted security/administration product. The tools will alert FSA the moment a protected file has been altered or tampered whether it is caused by a predatory hacker, a disgruntled employee, or simply an unintentional error. It will identify what was changed and provide a means to undo any damage. FSA has selected Tripwire as the standard software for intrusion detection.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

Network Intrusion Detection – RealSecure/Checkpoint

Description: To be determined.

Rationale: No published industry standard identified.

Physical Security – See OMB A130

Description: The Department of Education has published policy on the physical security of systems. This will be adopted by FSA until an FSA-specific policy is developed.

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture. Physical security requirements of each system will be described in the system's security plan.

Encryption – Router Encryption (DES3), Secure Socket Layer (128-bit), IPSec, Verisign (SSL) RSA Bsafe, RSA Bsafe Libraries, Sterling Commerce Connect Direct

Description: The standard for FSA will be DES3 encryption and RSA Public Key. AES was recently adopted as the new federal government encryption standard. The AES adoption is discussed in FIPS Pub 197.

As of March 2002, FSA applications that need to transmit information from one application hosted within the FSA data center that handles, stores and processes Privacy Act and confidential data, to another application hosted outside the FSA data center, should utilize router-level, hardware-based encryption to protect the confidentiality and integrity of in-transit information.

FSA applications transmitting information over open networks (via HTTP or FTP) to and from an application external to the originating data center must use SSL (Secure Socket Layer) data encryption to protect confidential information. SSL should also be used when confidential information is transmitted to and from a user external to the originating data center. The industry standard within the United States is 128-bit encryption and should be used. Outside the United States 40-bit encryption[1] should be used except in countries to which the United States allows higher bit levels of data encryption.

Owners of systems deployed before March 2002 will need to consider data encryption needs in preparing their system security plan. The risks of data being compromised and of not being in compliance with the Privacy Act will be weighed in deciding whether data will be encrypted.

Consult the Legal Department and/or the appropriate government agency any time encryption technology or encrypted information might cross government boundaries.

RSA BSAFE Libraries is used when developing applications that transfer data between web servers residing behind the firewall.

Rationale: DES is the federal standard for the encryption of data as set by OMB, and AES will be the new standard.

Hardware-based router level encryption provides a solution that will be available to any application hosted by the FSA data centers. For data centers receiving FSA data, this provides the most effective option from an implementation and operations perspective.

SSL encryption is the industry standard for application to end-user secure data transfer via the Internet. SSL implementation is well understood and supported by all major vendors of Internet and web application server products (IBM WebSphere products).

Virus Protection (Desktop) – McAfee VirusScan, Norton Enterprise Antivirus 7.1

Description: Platforms will have current anti-virus software installed and active to scan memory, boot sectors, email attachments, and files. Multi-layered anti-virus protection may require a combination of several products to provide adequate protection across multi-platforms.

**Norton Enterprise Antivirus 7.1 will be updated to Norton Enterprise Antivirus 2000 for FY2004 and FY2005.*

Rationale: Relevant standards are identified in the Department of Education Security Policy and the evolving FSA Security Architecture.

4.11 External Environment

Brief Description

This section addresses external environment technologies and standards outside the scope of the TRM. The external environment encompasses WAN transmission systems.

The FSA Wide Area Network (WAN) consists of several differing network topologies all standardized on the TCP/IP protocol. This maximizes the amount of network activity that can be delegated to the Internet and minimizes usage of costly dedicated circuits. Security is an issue for network traffic carried by private circuits or the internet. The following are consideration that should be made when implementing a WAN:

- *External Connections*, such as wide area networks (WANs), are divided into two parts. The first is trunk technology and switching. The customer generally purchases these services rather than investing in wide-area equipment and cable. The second is what the telephone industry refers to as the "local loop," meaning the reach from the central office to the business or residence. Often the customer owns these assets.

Target Standards

Target Standards: External Environment

	FY 2003	FY 2004	FY 2005
External Connections			
Technical Standard	Asynchronous Transfer Mode (ATM)	Asynchronous Transfer Mode (ATM)	Asynchronous Transfer Mode (ATM)
Technical Standard	Inverse Multiplexed Circuits (IMUX)	Inverse Multiplexed Circuits (IMUX)	Inverse Multiplexed Circuits (IMUX)

Technical Standard	Frame Relay	Frame Relay	Frame Relay
Technical Standard	Point-to-point	Point-to-point	Point-to-point
Technical Standard	Virtual Private Network (VPN)	Virtual Private Network (VPN)	Virtual Private Network (VPN)

Approved Standards

External Connections – Asynchronous Transfer Mode (ATM), Inverse Multiplexed Circuits (IMUX)

Description: The Virtual Data Center (VDC), in Meriden, CT., is the primary FSA internet presence. Two Internet Service Providers (ISPs) are used which allows load balancing of the connections with a Border Gateway Protocol (BGP). The BGP provides high level of reliability should a single ISP have a failure. The dual paths allow for tuning of inbound and outbound traffic as well.

FSA uses FTS 2001 vendors to provide WAN services. FSA uses Sprint for ATM, and dedicated point-to-point circuits and MCI for Frame Relay. All circuits require a minimum of 90 days lead time from the time the order is placed until the circuits are installed and tested. ISDN is used as a primary means of backup. The ISDN circuits are provided by the VDC and are connected directly into the back of the VDC provided routers.

The FTS 2001 vendors provide the topology requested and order the "last mile" from the Local Exchange Carrier (LEC) or a Competitive Local Exchange Carrier (CLEC). The LEC or CLEC install the data line connection into the requested facility. This portion of the connection should be equal to or greater than the size of the circuit being requested to allow bandwidth scalability.

- *Asynchronous Transfer Mode (ATM)* - Sprint is the provider for this service. With ATM the data may be passed around within the ATM cloud and not be redirected by a router that results in higher availability and flexibility. 3DES is normally deployed at the router level to secure Privacy Act data. ATM connections are expensive and should be well justified before being implemented. ATM has the highest available bandwidth of all topologies at 155 MBS. The premise equipment is provided by both Sprint and the VDC for this type of connection. Other topologies or data paths may be considered for backup, as required.
- *Inverse Multiplexed Circuits (IMUX)* – IMUX is a high bandwidth, high available data connection. It is used when high availably is required along with high bandwidth that is greater than 3 MBS and less than 12 MBS. IMUX is primarily used for data center to data center connections. Sprint provides FSA's IMUX dedicated circuits. The VDC provides the

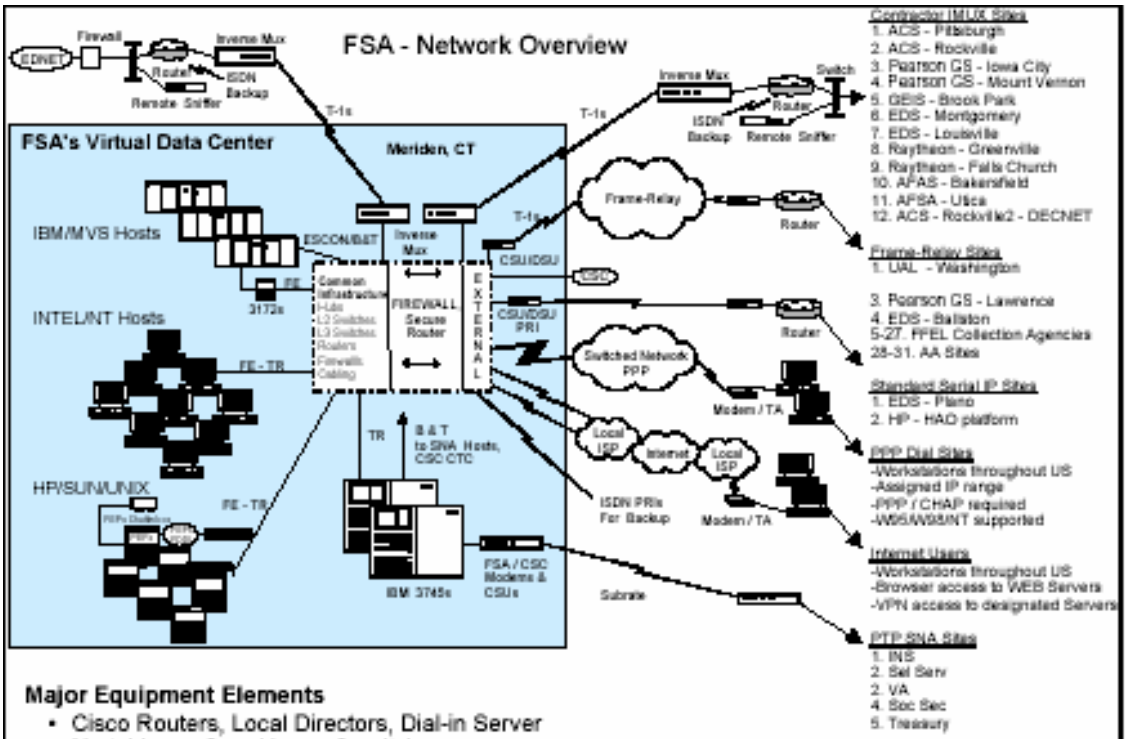
equipment for both ends of the connection, as well as, the ISDN backup circuits.

- *Frame Relay* - Frame Relay is used to support small offices of 50 full time people or less and where high availability or bandwidth is not required. The last mile for this type of connection is always a T-1, to allow for bandwidth growth. The CIR ordered for this type of connection is normally 56 KBS. If there is a need for additional bandwidth, the CIR can be increased to a full T-1 capacity. MCI is FSA's frame relay service provider. The VDC provides the equipment for both ends of the connection, as well as, the ISDN backup circuits.
- *Point-to-Point* – These types of dedicated services are either ordered as a 56 KBS or a 1.54 MBS. Due to the costs and bandwidth involved, normally only the T-1 service is ordered. Sprint is the service provider for point-to-point connections and the VDC provides the equipment for both ends, as well as the ISDN backup circuits. These circuits are also part of the IMUX solution when capacities of 3 MBS or greater is needed.

See Exhibit 4-2: FSA Network Overview

Rationale: Standards will be continually identified to meet FSA's strategy to consolidate its WAN and further refine its Infrastructure Architecture while maintaining the use of dedicated circuits and frame relay.

Exhibit 4-2: FSA Network Overview



Major Equipment Elements

- Cisco Routers, Local Directors, Dial-in Server
- Nortel Layer 2 and Layer 3 switches
- Check Point Firewalls, VPN
- Quick Eagle Inverse Multiplexers
- FSA FTS2001 MCI Frame-Relay, Sprint T1s and subrates
- Level 3 Communications, SNET/SBC ISPs
- SNET/SBC PRIs, multi-LEC BRIs

General Characteristics

- Isolated Network. Although Meriden is a milticustomer facility, the FSA Network is isolated from all other Meriden Networks. The FSA Network contains only FSA hosts and FSA-related transmission devices.
- High Availability. Good layer of redundancy, switched access for failures. Disaster recovery plans tested.
- Performance. Sufficient bandwidth to satisfy demand rates. Separate backup Network.
- Limited Access Permission. Default access is none. Access requires FSA permission.
- Protected Access. Enforce Network access rules with stateful firewalls, secure routers, security server. For designated Internet users, provide VPN (authentication, encryption, access restrictions, logging) access.
- Audited. Multiple audits per year. Includes penetration tests and Inspector General audits.
- Monitored. Includes intrusion detection, Global Management Center 7 x 24 event monitoring and performance reporting.
- ISO 9001 Certified. The Meriden Data Center, including the Meriden Network Team, is certified.

5 APPENDICES

Appendix A: Acronyms

Appendix B: Sources Referenced

Appendix C: Consistent Data Initiative

APPENDIX A: ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
ASP	Application Service Provider
BRM	Business Reference Model
CFO	Chief Financial Officer
CGM	Computer Graphics Metafile
COE	Common Operating Environment
CORBA	Common Object Request Broker Architecture
COTS	Commercial-Off-The-Shelf product
CRM	Customer Relations Management
CTI	Computer Telephony Integration
DBMS	Database Management System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOM	Document Object Model
DRM	Data Reference Model
EAI	Enterprise Application Integration
EDI	Enterprise Data Integration
EJB	Enterprise Java Beans
ERP	Enterprise Resource Management
ETL	Extract, Transform, And Load
FSA	Federal Student Aid
FTAM	File Transfer, Access, and Management
FTP	File Transfer Protocol
GOTS	Government-Off-The-Shelf product
GUI	Graphic User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol – Secure
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization (also known as the International Standards Organization)
ISP	Internet Service Provider

ITA	Integrated Technology Architecture
ITU-T	International Telecommunications Union–Telecommunications Standardization Sector
JDBC	Java Database Connectivity
JMS	Java Messaging Service
JNDI	Java Naming and Directory Interface
JSP	Java Server Pages
JVM	Java Virtual Machine
KPI	Key Performance Indicator
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MOFW	Managed Object Framework
MOM	Message Oriented Middleware
MPEG	Motion Picture Experts Group
MPEG2	Motion Picture Experts Group file format version 2
MPI2	Message Passing Interface 2
MSB	Minimum Security Baseline
ODBC	Open Database Connectivity
OLAP	Online Analytical Processing
OLTP	Online Transaction Processing
OMB	Office Of Management And Budget
OMG	The Object Management Group
PC	Personal Computer
PDA	Personal Digital Assistant
PPP	Point-to-Point Protocol
PRM	Performance Reference Model
PSTN	Public Switched Telephone Network
RACF	Resource Access Control Facility
RCS	Re-usable Common Services
RDBMS	Relational Database Management System
RFC	Request For Comment
RPC	Remote Procedure Call
RSA	Rivest, Shamir, Adleman
SGML	Standard Generalized Markup Language
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language

SRM	Service Reference Model
SSL	Secure Socket Layer
TOG	The Open Group
TOGAF	The Open Group Architectural Framework
TRM	Technical Reference Model
VPN	Virtual Private Network
WAN	Wide Area Network
WfMC	Workflow Management Coalition
XML	Extensible Markup Language
XSP	Any Service Provider (see ASP and ISP)

APPENDIX B: SOURCES REFERENCED

Documents:

- Enterprise Information Technology Architecture Framework: Business Drivers and Architecture Principles October 8, 1998
- FSA CIO Personnel
- FSA Data Management Policies and Procedures
- FSA Information Security General Minimum Security Baseline Standards
- FSA Information Technology Architecture Framework – Phase I
- FSA Software Engineering Handbook
- Office of Management and Budget (OMB) Circular A-130 Appendix III
- Office of Student Financial Assistance Guide to Information Security and Privacy
- Security Architecture
- Computer Services Corporation (CSC)
- Data Strategy
- FEAPMO Website

APPENDIX C: CONSISTENT DATA INITIATIVE

Federal Student Aid (FSA) is working to deliver consistent data to internal and external customers. In many FSA systems enhancement and legacy systems, it is presently difficult to obtain consistent information. The CIO Enterprise Data Architecture group formed a Consistent Data Team. In a joint effort with FSA's business and systems enhancement partners, the Consistent Data Team has developed high-level system overviews of FSA's primary systems and a Consistent Data (CD) Roadmap that depicts shared data responsibilities for each system in the FY2004 target vision. These resources are available in the Technology Handbook on FSA Net.

The CD Roadmap highlights the solution for establishing an enterprise environment with consistent data. With the CD Roadmap now in place, FSA has an opportunity to begin to design and build consistent data into its applications. The solutions recommended below, described in greater detail in the *Technology Handbook*, are provided to communicate what is required to achieve a consistent data oriented environment:

- Recommendation for system of record stewardship of data throughout the FSA lifecycle process.
- Identify points of data entry and update capabilities.
- Facilitate synchronization rules to enable single points of data entry and update.

The figure below summarizes the Phase I of the Consistent Data effort.